A SYSTEMATIC REVIEW OF LITERATURE GAPS IN CLOUD CYBERSECURITY

Article type: Review
Corresponding author:
Tristan Barbara
tristanbarbara@hotmail.com

Tristan Barbara [1]

[1] University of Malta, Malta

Abstract

Purpose: This study aims to serve as a reference point for identifying gaps in cloud computing cybersecurity (CCCS) and the associated cloud computing cybersecurity risks (CCCRs). Furthermore, it seeks to provide guidance on future research directions required to address these gaps. **Methodology:** The study employs a systematic literature review of the Google Scholar and Scopus databases, adhering to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines for study selection. Through this process, eleven studies were identified and analysed. **Findings:** The themes identified regarding CCCRs centred on the weakening of the confidentiality, integrity, and availability (CIA) triad, resulting in less robust cybersecurity infrastructures. The reviewed literature showed consistent perspectives on CCCS, highlighting the need for further research to deepen understanding of this technology. Accordingly, the study identifies a gap in the existing research, which generates uncertainty among industry practitioners and hinders the adoption of cloud computing (CC). **Originality/value:** The findings complement recent reviews indicating that digital transformation improves efficiency while increasing cybersecurity risks and requiring organizational resilience frameworks. Unlike studies focusing on technological infrastructure and security gaps in cloud environments, this research provides a human–organizational perspective by integrating engagement, life satisfaction, and sufficiency–necessity logic to explain performance.

Keywords: cloud computing cybersecurity, cloud computing, cloud computing cybersecurity risk, cybersecurity, emerging technologies
JEL Codes: O33, L86, M15

How to cite this article: Barbara, T. (2026). A systematic review of literature gaps in cloud cybersecurity. *Peruvian Journal of Management*, (3), 135-160. https://doi.org/10.26439/pjm2026.n003.8142.
Article history: Received: July 21, 2025. Accepted: February 10, 2026.
Published online: April 15, 2026.

UNA REVISIÓN SISTEMÁTICA DE LAS BRECHAS EN LA LITERATURA SOBRE CIBERSEGURIDAD EN LA NUBE

Resumen

Objetivos: El objetivo de esta investigación es servir como punto de referencia para identificar las brechas en la Ciberseguridad de la Computación en la Nube (CCCS) y los Riesgos de Ciberseguridad de la Computación en la Nube (CCCRs) que estas presentan. A través de ello, el estudio busca proporcionar orientación sobre qué investigaciones futuras deberían llevarse a cabo para abordar dichas brechas. **Metodología/Diseño:** El estudio emplea una metodología de revisión sistemática de la literatura, utilizando las bases de datos Google Scholar y Scopus, y siguiendo las directrices de los Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) para la selección de estudios. Mediante este proceso se identificaron y analizaron once estudios. **Resultados:** La temática identificada en relación con los CCCRs giró en torno al debilitamiento de la tríada CIA (Confidencialidad, Integridad y Disponibilidad), lo que conduce a infraestructuras de ciberseguridad más frágiles. Los temas tratados por la literatura analizada fueron coherentes en sus perspectivas sobre la CCCS, lo que evidencia la necesidad de más investigaciones para profundizar en la comprensión de esta tecnología. El estudio, por tanto, señala la necesidad y la carencia de este tipo de investigaciones, lo que genera un nivel de incertidumbre entre los profesionales del sector que dificulta la adopción de la computación en la nube. **Originalidad/Valor:** Los hallazgos complementan revisiones recientes que muestran que la transformación digital mejora la eficiencia, pero incrementa los riesgos de ciberseguridad y exige marcos de resiliencia organizacional. A diferencia de los estudios centrados en la infraestructura tecnológica y las brechas de seguridad en entornos de computación en la nube, esta investigación aporta una perspectiva humano-organizacional al integrar el compromiso, la satisfacción con la vida y la lógica de suficiencia-necesidad para explicar el desempeño.

Palabras clave: Ciberseguridad en la computación en la nube; computación en la nube; riesgo de ciberseguridad en la computación en la nube; ciberseguridad; tecnologías emergentes.
Códigos JEL: O33, L86, M15

1. INTRODUCTION

Cloud computing (CC) has transformed how organisations access and manage computing resources by enabling remote, Internet-based operations. Scholarly and industry definitions demonstrate broad consensus regarding its core characteristics: scalability, efficiency, and on-demand availability. Authoritative institutions such as the National Institute of Standards and Technology (Mell & Grance, 2011), Amazon Web Services, Inc. (n.d.), the Cloud Security Alliance (Spelman, 2015), and IBM (Susnjara & Smalley, n.d.) emphasise these elements in their conceptualisations.

1.1 Literature Review

1.1.1 Defining Cloud Computing

IBM defines CC as "on-demand access, via the Internet, to computing resources hosted at a remote data centre managed by a cloud services provider" (Bennasar et al., 2017). This model, typically subscription-based or pay-per-use, allows resources to scale according to demand (Spelman, 2015) and offers a cost-effective alternative to maintaining physical servers and data centres (Amazon Web Services, Inc., n.d.). Similarly, Microsoft (n.d.) describes CC as "the delivery of computing services over the internet," enabling users to pay only for what they consume while improving operational efficiency. Within the literature, CC is widely recognised as an emerging technology due to its rapid evolution, innovative character, and socioeconomic influence (Xu, 2010; Khan et al., 2011; Ganne, 2022; Hernandez, 2022). It integrates environments based on LANs, WANs, VPNs, and APIs to create unified virtual infrastructures. These architectures combine flexibility and performance, establishing CC as a key driver of digital transformation.

1.1.2 Defining Cybersecurity

Within this dynamic landscape, cyber risk is broadly defined as "any risk of financial loss, disruption or damage to an organisation's reputation resulting from a failure of its information technology systems" (Institute of Risk Management, 2014). When comparing definitions of cybersecurity, given by Craigen et al. (2014), and the National Institute of Standards and Technology (n.d.), it can be noted that, despite temporal differences, they converge on the protection of digital assets and infrastructure.

1.1.3 Interrelation Between Cybersecurity and CC

When such risk occurs in cloud environments, it is referred to as cloud computing cybersecurity risk (CCCR). Given the pace of technological advancement and the inherent uncertainty of emerging technologies—characterised by radical novelty, rapid growth, and socioeconomic impact—continuous research is required to identify existing knowledge gaps (Rotolo et al., 2015).

Cloud computing cybersecurity (CCCS), defined as the protection of cloud processes and systems against threats that compromise confidentiality, integrity, and availability (CIA), evolves rapidly and unpredictably (National Institute of Standards and Technology, n.d.). This constant evolution makes it difficult for both individual and organisational users to remain current with the latest vulnerabilities, such as zero-day attacks (Bilge & Dumitraş, 2012), as well as with emerging paradigms such as microservices and serverless computing, which allow scalable and infrastructure-free development (Douglis & Nieh, 2019; Li et al., 2023). Similarly, the emergence of related technologies, including artificial intelligence (AI) and the Internet of Things (IoT), has intensified both the complexity and exposure of cloud ecosystems.

1.2. Formulation of the Research Questions

Despite the growing body of research on CCCS and CCCRs, systematic analyses of current and emerging gaps in this domain remain limited. Although prior studies, such as that of Nobanee et al. (2023), have examined cybersecurity risks associated with emerging technologies, few have undertaken a systematic analysis of current and prospective gaps

within the domain of CCCS. As emerging technologies continue to evolve rapidly, there is a sustained need to map the state of knowledge and identify areas requiring further investigation. To guide future studies on literature gaps warranting additional research, this study addresses the following research question: What research gaps in CCCS are identified in existing literature review studies?

By emphasising governance and management dimensions often neglected in technically oriented research, this study aims to contribute to a more comprehensive understanding of the organisational and human factors influencing cybersecurity practices in cloud-based environments.

2. METHODS

2.1. Research Strategy and Criteria

The structure of this paper follows the schematic research methodology steps presented in Table 1, which outlines the sequential approach adopted throughout the study. The research consistently employs the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure methodological transparency and replicability.

A systematic literature review (SLR) was conducted to examine the principal issues highlighted in the contemporary literature on CCCS and to identify future research perspectives. The aim was to obtain a balanced and representative overview of scholarly debates within the field. The SLR method was selected as the most appropriate approach to achieve these objectives, as enables the structured and unbiased collection, appraisal, and synthesis of existing evidence.

Table 1

Schematic Research Methodology Steps

Step number	Step description
1	Delineating the Primary Research Inquiries
2	Preliminary Literature Review
3	Determining Research Questions for The Systematic Literature Review
4	Following the PRISMA Flow Diagram and Checklist for the data collection process
	4.1 Define inclusion and exclusion criteria, specify databases used.
	4.2 Determine search strategy (search terms etc.)
	4.3 Determine measures taken to avoid bias in the data collection process.
	4.4 Follow this strategy to acquire the first set of unfiltered results.
5	Screening the results based on the PRISMA method
	5.1 Determine criteria for assessing whether each study is eligible, assess, and explain reasons for exclusions.
	5.2 Determine criteria for classifying eligible studies and classify them accordingly.
	5.3 Create a Diagram/Table showing the initial results from the search, and the final results after filtering the studies according to the eligibility criteria.

(*continues*)

(*continued*)

Step number	Step description
6	Presenting the results based on the classifications set for the eligible studies
7	Answering the research questions from the final results obtained
8	Determining gaps in literature and potential future research suggestions
9	Discussing the conclusions resulting from this study

By adopting this structured approach, the review provides readers with a transparent, comprehensive, and precise account of the study's objectives, methods, and findings (Page et al., 2021). As noted by Nightingale (2009), systematic reviews are valuable because they enable researchers to produce a rigorous and impartial synthesis of the available literature on a given topic. The application of this method enhances the accuracy and reliability of the results by incorporating all studies that satisfy the inclusion criteria, thereby minimising bias and ensuring that the evidence base is neither under-represented nor distorted.

To ensure proper execution, this study followed the PRISMA 2020 checklist and its 27-item statement. The primary objective was to obtain a comprehensive understanding of existing gaps in the CCCS literature. Accordingly, only scholarly works explicitly addressing this topic were included. To maintain relevance, specific inclusion and exclusion criteria were established, as summarised in Table 2.

Table 2

Inclusion and Exclusion Criteria and Their Justification

No.	Inclusion criteria	Exclusion criteria	Reasons
1	The study must be freely accessible in its full version, either as an open-access publication, or through the resources provided by the University of Malta.	Studies that are inaccessible due to a paywall will be omitted.	By restricting inclusion to papers that are open access or accessible through University of Malta student resources, this study enables a thorough examination of the selected literature and ensures the replicability of both the research process and its findings.
2	The study should be written in English.	Any studies not written in English.	By limiting inclusion to studies published in English, the study ensures accurate comprehension of the selected literature and minimises the risk of misinterpretation arising from translated texts.
3	Literature which discusses the relationship between cyber security and cloud computing.	Any literature that does not address the relationship between cyber security and cloud computing.	This ensures that included studies are relevant to this study.

(*continues*)

(*continued*)

No.	Inclusion criteria	Exclusion criteria	Reasons
4	The study's title must contain both ("cloud computing" OR "cloud-based" OR "cloud") and ("cybersecurity" OR "cyber security" OR "security").	Studies that do not address both topics, or that examine only one topic in isolation without reference to the other.	This is to ensure that the study discusses both cyber security and cloud computing within the research study.
5	Literature published in 2023, up to and including July.	Literature published before 2023 or after July 2023.	Because cloud computing and cybersecurity are rapidly evolving fields, this ensures that the most recent developments are considered.
6	The study must be a literature review.	Studies that are not literature reviews or that do not describe their methodology.	Analyzing literature reviews enables the assessment of the conclusions drawn by these studies and the sources they encompass. Requiring a clearly described methodology helps ensure the quality of the included reviews.

Two databases, Google Scholar and Scopus, were employed as primary sources to retrieve relevant studies. Their selection was based on professional consultation with colleagues, who recommended them as comprehensive and up-to-date sources for research in information systems and cybersecurity. The scope was limited to these two databases due to time and resource constraints, including restricted access to subscription-based databases. Despite these limitations, the combination of Scopus and Google Scholar offered a sufficiently comprehensive foundation for identifying the primary literature for this study.

Given the dynamic nature of CCCS, in which significant advances occur each year, only material published between January and July 2023 was included. This timeframe ensured that the review reflected recent developments in the field. Moreover, the study focused exclusively on literature reviews, as such works synthesize findings from numerous primary studies and provide an aggregated perspective on the state of knowledge.

Based on the above criteria, the following search strategies were applied:

For Google Scholar the following search string was used:

allintitle: ("cloud computing" OR "cloud-based" OR "cloud") ("cybersecurity" OR "cyber security" OR "cyber" OR "security")

The results included various types of research outputs; however, filtering was applied to retain only peer-reviewed articles published in 2023.

For Scopus the following search string was used:

TITLE (("cloud computing" OR "cloud-based" OR "cloud") AND ("cybersecurity" OR "cyber security" OR "cyber" OR "security")) AND PUBYEAR = 2023 AND (LIMIT-TO

(DOCTYPE , “re”)) AND (LIMIT-TO (EXACTKEYWORD , “Cloud Computing”) OR LIMIT-TO (EXACTKEYWORD , “Cloud-computing”) OR LIMIT-TO (EXACTKEYWORD , “Security”) OR LIMIT-TO (EXACTKEYWORD , “Cloud Security”) OR LIMIT-TO (EXACTKEYWORD , “Cybersecurity”) OR LIMIT-TO (EXACTKEYWORD , “Cyber Security“) OR LIMIT-TO (EXACTKEYWORD , “Review”))

This search yielded eight results in Scopus, a manageable number that allowed for precise screening in accordance with the established inclusion criteria. The Google Scholar search produced a larger set of records, from which only eligible peer-reviewed studies were retained.

For both databases, all identified records were manually reviewed to ensure full compliance with the specified criteria. The screening process verified that each selected study was available in full text, published within the required timeframe, written in English, and explicitly addressed the relationship between cloud computing and cybersecurity.

2.2. Screening Process

The quality and eligibility of the search results generated by the defined terms were assessed manually by a single reviewer, without the use of automated software. Each record retrieved from the databases was evaluated through a systematic process to determine its suitability for inclusion in the study.

Initially, duplicate studies were identified and removed. When a paper appeared in multiple sources, the most recent version was retained. An eligibility assessment was then conducted in accordance with the inclusion and exclusion criteria listed in Table 2. At this stage, each article was confirmed to be written in English, available in full text, accessible either publicly or through resources provided by the University of Malta, and to explicitly address the relationship between cybersecurity and cloud computing. Only studies meeting all these conditions were retained for the final dataset used in this review.

2.3. Data Extraction Process

This subsection describes the approach used to extract and systematize information from the selected studies. Each article meeting the eligibility criteria was reviewed in full, and detailed notes were compiled on the main themes addressed, the arguments presented, and the conclusions reached. These observations were summarised in Table 3, which lists the specific topics covered in each study.

A similar mapping process was conducted to document the recommendations and future research directions proposed by the authors, as summarised in Table 4. Together, these two tables enabled a structured and consistent comparison of the reviewed literature and supported the subsequent synthesis of findings.

For each study included in the dataset, key information was extracted, including the title and authors, the central research focus and motivation, recommendations for further investigation, and whether the paper proposed concrete solutions to strengthen CCCS or merely identified unresolved challenges. All data extraction procedures were performed manually by a single researcher to maintain methodological consistency throughout the process.

2.4. Assessing Risk of Bias in the Included Research Studies

Assessing risk of bias is an essential component of literature analysis, as it ensures the overall quality and credibility of the reviewed studies. During the screening stage, each candidate paper was briefly evaluated to identify potential sources of bias.

Bias mitigation was primarily achieved through the inclusion of Criterion 5, which required that all included studies be literature reviews conducted using a sound and transparent methodology. The adoption of this structured approach inherently reduces subjectivity, thereby increasing confidence that the selected studies present a lower risk of bias.

Additionally, only studies authored by multiple researchers were included, as collaborative research generally enhances internal verification. The presence of more than one author helps identify and correct potential weaknesses or biases, improving the overall reliability of the published work.

2.5. Data Synthesis Methodology

The data synthesis process followed a structured and systematic approach. Each paper included in the final dataset was thoroughly reviewed, and key information was extracted regarding the topics addressed, the principal arguments presented, and the recommendations for future research.

After the initial extraction phase, two synthesis tables were constructed to facilitate analysis. These tables mapped the studies according to (i) the topics discussed and (ii) the future research directions identified by their authors. This dual mapping enabled the categorisation of the literature by both thematic focus and by suggested research trajectories, providing a clearer understanding of collective trends and gaps in the field.

This systematic synthesis also generated the evidence required to answer the research questions formulated for this study. All references and bibliographic data were organised and managed using RefWorks, which supported storage and tracking of the reviewed primary literature.

2.6. Measures for Avoiding Bias in the Data Collection and Analysis Phases

To address potential bias arising from the use of a single reviewer, several measures were implemented to minimize this risk. First, the PRISMA checklist was rigorously followed during both the data collection and the analysis phases. This predefined framework reduced ad-hoc decision-making during both phases, ensuring a structured, transparent, and replicable workflow.

A standardised extraction process was also implemented through Tables 3 and 4, in which identical categories of information were recorded for each study. Throughout the process, a decision log was maintained to document borderline cases, and uncertainties were discussed with a supervisor to reduce subjective judgement.

All extracted information was systematically gathered from the Results, Discussion, Conclusions, and Future Recommendations sections of each reviewed paper. Care was taken to ensure that all entries were transcribed faithfully, maintaining the wording and intent of the original authors to avoid misinterpretation.

These systematic and impartial procedures ensured that all extracted data accurately reflected the content and meaning of the original research, thereby mitigating the limitations inherent in a single-reviewer design.

3. RESULTS

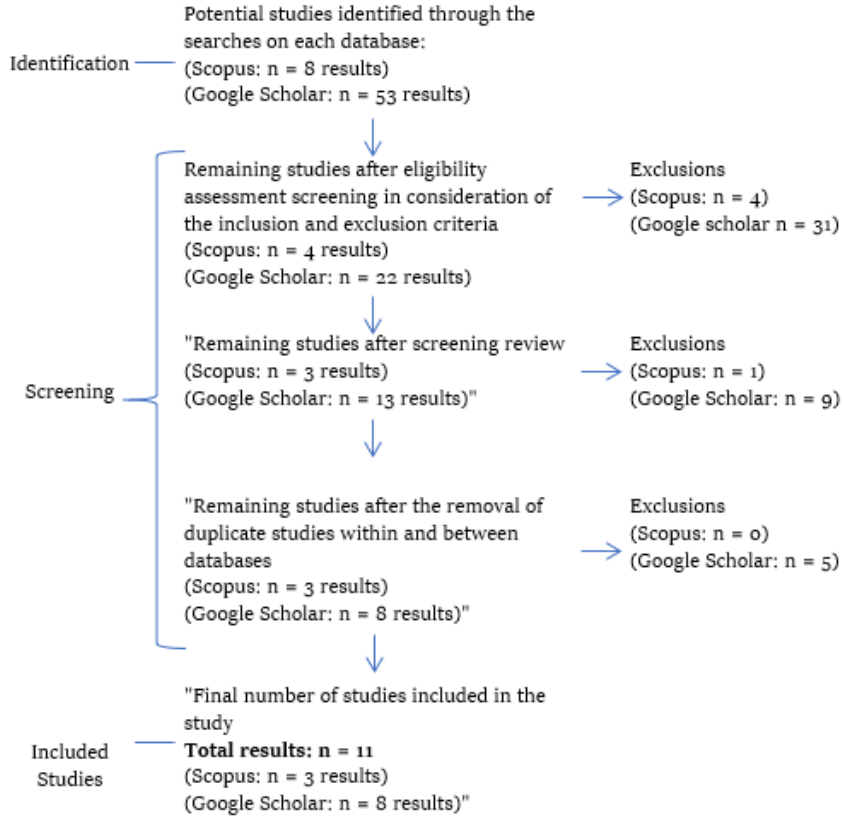
Selection of Literature

The literature selection process is illustrated in Figure 1, which summarises the sequence of identification, screening, and inclusion stages. The initial searches conducted in Google Scholar and Scopus produced a combined total of 53 records (45 from Google Scholar and 8 from Scopus). Each study was manually screened against the inclusion and exclusion criteria defined in Table 2, ensuring alignment with the study's scope.

After duplicates and ineligible papers were removed, 11 studies were retained for detailed analysis—eight sourced from Google Scholar and three from Scopus. These studies collectively form the dataset for this review.

Figure 1

Flow Diagram Depicting the Screening Process of the Identified Studies



3.2. Analysis of Results

The eleven selected studies were analysed in depth, and key information was extracted to address the research questions. Using Tables 3 and 4, each paper was categorised according to the main topics discussed and the proposed future research directions.

From this synthesis, six core thematic clusters emerged from the literature. Table 3 provides an overview of the most frequently addressed topics across the studies.

Table 3

Topics Discussed by Each Identified Study

Paper	Topic discussed by the study					
	The need for more robust and better understanding of cryptographic algorithms for the encryption of cloud data	Lack of focus on the security of cloud-based Workflow Management Systems	The lack of literature discussing Cloud Battery Management Systems (CBMS)	Challenges faced by organisations in their adoption and use of cloud computing	Existing defensive solutions and tools for improving the security of microservice architectures and cloud-native systems	The integration of cloud computing systems with emerging technologies (such as IoT and AI)
(Soveizi et al., 2023)		Highlights the lack of literature on cloud-based workflow management systems				
(Can et al., 2025)	Calls for improved cryptographic algorithms					
(Naseri et al., 2023)			Highlights a lack of literature relating to CBMS			
(Komar et al., 2023)				Highlights factors being major barriers to CC adoption		
(Dawson et al., 2023a)	Highlights the importance of encryption in CCCS					

(*continues*)

(*continued*)

Paper	Topic discussed by the study					
	The need for more robust and better understanding of cryptographic algorithms for the encryption of cloud data	Lack of focus on the security of cloud-based Workflow Management Systems	The lack of literature discussing Cloud Battery Management Systems (CBMS)	Challenges faced by organisations in their adoption and use of cloud computing	Existing defensive solutions and tools for improving the security of microservice architectures and cloud-native systems	The integration of cloud computing systems with emerging technologies (such as IoT and AI)
(Jha et al., 2023)				Highlights low CCCS awareness and weak methodological rigour in existing research		
(Rahaman et al., 2023)					Noted how orchestration layers and runtime environments were insufficiently protected	
(Pawlicki et al., 2023)						Discusses the cybersecurity of CC, Edge Computing, and IoT
(Minna & Massacci, 2023)					Identifies a lack of real-world studies on microservice architectures and cloud-native systems	
(Dawson et al., 2023b)	Highlights the importance of encryption in CCCS					
(Surianarayanan & Chelliah, 2023)						Discuss increased vulnerabilities in using CC with Emerging technologies

Table 4

Table of Identified Future Recommendations for Each Identified Study

Paper	Future directions identified							
	Further development of cryptographic algorithms (such as Genetic and DNA cryptography) and their application to emerging technologies	Further research on CBMS cyber security	The need for the establishment of better regulatory standards and further developments of frameworks to be followed for better cyber security within the cloud	Further research on the integration of emerging technologies (such as AI, IoT, Cloud Computing, and Edge Computing) for better cyber security	Further research on various security issues in cloud computing	Further research on sustainable cloud-based infrastructures	Future research should focus on optimizing serverless computing architectures	Further developments on cyber risk management tools to keep up with the evolution of cyber risks
(Soveizi et al., 2023)			Highlights the need for more robust operational frameworks for cloud-based infrastructures					
(Can et al., 2025)	Proposes non-linear cryptographic tools such as DNA cryptography							
(Naseri et al., 2023)	Notes the importance of encryption in CBMS Cloud Security	Notes further research is required on CBMS CCCS	Requests more research to be done on tools for enhancing CCCS throughout the CC use lifecycle	Requests further research on the integration of CC with Emerging Technologies				

(*continues*)

(*continued*)

Paper	Future directions identified							
	Further development of cryptographic algorithms (such as Genetic and DNA cryptography) and their application to emerging technologies	Further research on CBMS cyber security	The need for the establishment of better regulatory standards and further developments of frameworks to be followed for better cyber security within the cloud	Further research on the integration of emerging technologies (such as AI, IoT, Cloud Computing, and Edge Computing) for better cyber security	Further research on various security issues in cloud computing	Further research on sustainable cloud-based infrastructures	Future research should focus on optimizing serverless computing architectures	Further developments on cyber risk management tools to keep up with the evolution of cyber risks
(Komar et al., 2023)			Highlights the need for strong access control, authentication, and adherence to regulatory standards	Requests further research on the integration of CC with Emerging Technologies	Highlights the need for strong access control, authentication, and adherence to regulatory standards	Emphasises the importance of the ongoing evolution of riskmanagement tools	The need for better CC operational frameworks	Emphasises the importance of the ongoing evolution of riskmanagement tools
(Dawson et al., 2023a)	Call for advancements in non-linear cryptographic algorithms				The need to demystify CCCS for greater adoption			
(Jha et al., 2023)	Majority of reviewed studies relied on encryption							
(Rahaman et al., 2023)								Highlights the need for cloud-tailored cyber risk management tools to be developed

(*continues*)

(*continued*)

Paper	Future directions identified							
	Further development of cryptographic algorithms (such as Genetic and DNA cryptography) and their application to emerging technologies	Further research on CBMS cyber security	The need for the establishment of better regulatory standards and further developments of frameworks to be followed for better cyber security within the cloud	Further research on the integration of emerging technologies (such as AI, IoT, Cloud Computing, and Edge Computing) for better cyber security	Further research on various security issues in cloud computing	Further research on sustainable cloud-based infrastructures	Future research should focus on optimizing serverless computing architectures	Further developments on cyber risk management tools to keep up with the evolution of cyber risks
(Pawlicki et al., 2023)					Highlights the importance of managing humancentred risks			
(Minna & Massacci, 2023)	w				Highlights the need for better defence mechanisms that can keep up with the evolving Highlights the need for better defence mechanisms that can keep up with the evolving landscape of cloud native and microservice based systems.			

(*continues*)

(*continued*)

Paper	Future directions identified							
	Further development of cryptographic algorithms (such as Genetic and DNA cryptography) and their application to emerging technologies	Further research on CBMS cyber security	The need for the establishment of better regulatory standards and further developments of frameworks to be followed for better cyber security within the cloud	Further research on the integration of emerging technologies (such as AI, IoT, Cloud Computing, and Edge Computing) for better cyber security	Further research on various security issues in cloud computing	Further research on sustainable cloud-based infrastructures	Future research should focus on optimizing serverless computing architectures	Further developments on cyber risk management tools to keep up with the evolution of cyber risks
(Dawson et al., 2023b)	Call for advancements in non-linear cryptographic algorithms				The need to demystify CCCS for greater adoption			
(Surianarayanan & Chelliah, 2023)				Highlights that expanding IoTcloud ecosystems require adaptive and robust security frameworks capable of addressing emerging CCCR				

The methodological quality of the selected studies was assessed using a simplified checklist adapted from Kitchenham and Charters (2007). The checklist evaluated seven criteria: clarity of the research questions, search strategy, inclusion/exclusion criteria, data extraction procedures, description of included studies, discussion of limitations, and coherence between data and conclusions. Each criterion was rated as Yes, Partial, or No, with a simplified score assigned according to its outcome. Criteria rated "Yes" received a score of 1, those rated "Partial" received 0.5, and those rated "No" received 0. The results of this quality appraisal were then summarised in Table 5. Papers with a combined score of 3.5 or less were classified as "Low Quality," those scoring from 4 to 5.5 as "Medium Quality," and those scoring from 6 to 7 as "High Quality." Table 5 presents the final aggregated scores and the resulting quality classification for each included study.

Table 5

Adapted Quality Assessment of Included Studies Based on Kitchenham and Charters (2007)

Paper	Average score	Overall quality
(Soveizi et al., 2023)	6.5	High quality
(Can et al., 2025)	5	Medium quality
(Naseri et al., 2023)	4	Medium quality
(Komar et al., 2023)	2	Low quality
(Dawson et al., 2023a)	4.5	Medium quality
(Jha et al., 2023)	3	Low quality
(Rahaman et al., 2023)	5.5	Medium quality
(Pawlicki et al., 2023)	7	High quality
(Minna & Massacci, 2023)	7	High quality
(Dawson et al., 2023b)	6	High quality
(Surianarayanan & Chelliah, 2023)	5.5	Medium quality

3.2.1. Cryptographic Approaches for Enhancing Cloud Data Security

Five out of the 11 included studies identified encryption as a core component for improving CCCS. The study of Can et al. (2025) focuses on DNA cryptography, an emerging bio-inspired approach that combines classical algorithms with biological DNA concepts to achieve faster and more energy-efficient encryption. Complementing this view, Dawson et al. (2023a, 2023b) conducted two systematic reviews assessing the performance of security algorithms in cloud environments. Their findings reaffirm encryption as "the best approach to ensure cloud security" and underscore that many vulnerabilities stem from compromises of the CIA triad. Both studies call for advances in nonlinear cryptographic algorithms, which offer unpredictable execution times and greater resistance to modern attacks compared to traditional linear schemes. Jha et al. (2023) also remarks on the use of encryption for CCCS. Their study noted that 45 % of all the reviewed studies relied on encryption as their primary security mechanism. Naseri et al. (2023) note that although encryption is essential for securing CBMS, it is insufficient on its own in such cyber-physical cloud environments.

3.2.2. Security Gaps in Cloud-Based Workflow Systems

Soveizi et al. (2023) investigate the increasing reliance on data-intensive processes within business operations and how these challenge the adoption of CC. Their work underscores that security and privacy concerns remain the primary deterrents for organisations—particularly those handling sensitive information—to fully adopting CC.

Through a systematic review, the authors identify several underexplored areas in the literature on cloud-based business and scientific workflows. They observe that most existing research concentrates narrowly on workflow modelling, neglecting critical stages such as monitoring, analysis, and adaptation. Moreover, they report an absence of reliable and scalable approaches for detecting, preventing, and responding to breaches throughout the workflow lifecycle. The study concludes that current workflow management systems do not adequately support both cloud infrastructure and end-to-end security requirements. Accordingly, Soveizi et al. (2023) call for future research to design integrated workflow security frameworks capable of dynamically monitoring and mitigating risks across the entire lifecycle, thereby bridging a key gap in CCCS implementation.

3.2.3. Cybersecurity Risks in Cloud Battery Management Systems (CBMS)

Naseri et al. (2023) explore the convergence of Battery Management Systems (BMSs) with cloud infrastructure, resulting in CBMSs, defined as "a cyber-physical system with connectivity between the physical BMS and a cloud-based virtual BMS, realised through a communication channel such as the Internet of Things." CBMSs enhance performance, scalability, and efficiency—particularly for electric vehicles (EVs)—yet their integration introduces critical cybersecurity risks that threaten CIA. This study uniquely identified vulnerabilities arising from both in-vehicle and extra-vehicle communications, including data theft, compromised GPS privacy, accelerated battery degradation, and potentially life-threatening safety failures. The authors conclude that although CBMSs offer promising industrial potential, their safe and reliable deployment ultimately depends on bridging current gaps in cybersecurity regulation and technical resilience.

3.2.4. Organisational Barriers to Cloud Adoption

The adoption of CC offers clear organisational benefits; however, its uptake is hindered by persistent security, regulatory, and operational challenges. Komar et al. (2023) highlight data protection, regulatory compliance, and vendor lockin as major barriers, stressing the need for robust access control, authentication, and adherence to regulatory standards such as the General Data Protection Regulation (GDPR). Jha et al. (2023) add that limited cybersecurity awareness and weak methodological rigour in existing studies undermine confidence in current security models. Although encryption is widely used, its effectiveness depends on continuous innovation to address evolving threats. Both studies indicate that technical safeguards alone are insufficient for secure cloud adoption. Effective implementation depends equally on governance structures, user awareness, standardised frameworks, and the ongoing evolution of technologies and riskmanagement tools.

3.2.5. Defensive Mechanisms for Cloud-Native and Microservice Architectures

CC and microservice architectures introduce complex security challenges that current research has not yet fully resolved. In their study, Rahaman et al. (2023) reviewed existing defence mechanisms, particularly static analysis tools, and found that most work focused

on containerlevel vulnerabilities, addressing attacks such as DDoS, CSRF, SQL injection, XSS, and replay attacks. They argue that more advanced static analysis solutions are needed to detect and mitigate emerging adversarial threats.

Minna and Massacci (2023) complement this perspective by examining tools for securing microservice runtime environments, identifying major gaps in the orchestration architectural layer, security policy verification, and microservice architectural resilience. They highlight insufficient testing of deployed systems, poor reproducibility in security experiments, and a lack of "security studies in the wild." Together, these findings point to the need for systematic, validated, and reproducible defence mechanisms capable of keeping pace with the evolving threat landscape found in cloudnative and microservicebased systems.

3.2.6. Integration of Cloud Systems With Emerging Technologies

The integration of CC with emerging technologies such as IoT and edge computing systems has not only created new benefits, introduced common vulnerabilities that remain underaddressed in current research. Pawlicki et al. (2023) catalogue frequent attacks, including DoS/DDoS, eavesdropping, MitM, and malware, and recommend AI/ML-enhanced intrusion detection, encryption, monitoring tools, and traditional defences such as firewalls and antivirus software. They also highlight the importance of managing human-centred risks through employee screening, robust access control, and standardised cybersecurity frameworks.

Surianarayanan and Chelliah (2023) similarly emphasise that integrating IoT with cloud platforms introduces additional weaknesses despite benefits such as centralised security management. They note that IoT systems remain vulnerable to manual errors, insider threats, physical attacks, and risks from thirdparty providers. Both studies conclude that expanding IoTcloud ecosystems require adaptive and robust security frameworks capable of addressing emerging and increasingly complex cyber threats.

4. DISCUSSION

4.1. Analysis of the Findings

CCCS is a broad domain, with researchers addressing different aspects. The results identified numerous gaps in the literature that warrant further investigation. The theme of cyber risks and threats within CC commonly revolves around the weakening of the CIA triad, thereby leading to less secure cybersecurity infrastructures.

One of the most frequently discussed topics in the included studies is encryption as a tool for enhancing CCCS. Five of the eleven papers emphasised encryption as a core mechanism for CCCS; however, much of the discussion also focused on its limitations. Some studies attempt to address these limitations by proposing nonlinear cryptographic approaches such as DNA cryptography (Can et al., 2025) and by calling for broader advances in nonlinear cryptographic algorithms (Dawson et al., 2023a, 2023b). Nevertheless, many of these proposals remain largely conceptual, with limited practical applicability and scarce supporting literature. Particularly in light of the increasing global adoption of CC, highly specific cybersecurity solutions may not be viable for a broad range of service users. This concern is further emphasised by Soveizi et al. (2023), who identify persistent gaps in end-to-end workflow security. Such gaps significantly deter organisational adoption of CC and underscore the need for security frameworks that cover the entire lifecycle of a CC use case while dynamically detecting and mitigating CCCS threats. A related line of inquiry

is presented by Naseri et al. (2023) in their discussion of CBMS. Although more specific in scope, this study likewise highlights the need for further research on tools capable of enhancing CCCS throughout its operational lifecycle.

Research on cloud-native and microservice architectures also reveals significant shortcomings in existing defence mechanisms. Rahaman et al. (2023) show that most tools remain focused on container-level vulnerabilities, leaving orchestration layers and runtime environments insufficiently protected against emerging adversarial threats. Complementing this, Minna and Massacci (2023) identify major weaknesses in security policy verification, architectural resilience, and the reproducibility of security experiments, revealing a lack of real-world "security studies in the wild". Two studies—Surianarayanan and Chelliah (2023) and Pawlicki et al. (2023)—further underscore the increased vulnerabilities associated with integrating CC with emerging technologies such as IoT and edge computing systems, many of which have not yet been adequately addressed in the current literature. These findings also highlight the need for further research on this topic.

Beyond the technical aspects of CCCS, this study identifies the need for improvements at organisational and human levels. Komar et al. (2023) point to regulatory pressures, data protection requirements, and vendor lock-in as key barriers, while Jha et al. (2023) highlight low CCCS awareness and weak methodological rigour in existing research. These studies show, that apart from technical measures, effective cloud security requires stronger governance, standardised frameworks, and improved user and organisational capabilities. The limited volume of research on CCCS underscores the need for further studies on improving organisational awareness of CCCS and on establishing common governance and regulatory frameworks for the adoption and safe use of CC.

Based on the analysed literature, there is clear agreement that further research is required for academics and industry professionals to enhance their understanding of this technology. The scarcity of such research creates a level of uncertainty amongst industry practitioners that hinders the adoption of CC. Both papers by Dawson et al. (2023a, 2023b), as well as those by Komar et al. (2023) and Jha et al. (2023), outline how security-related uncertainties surrounding CC establish a core barrier to its faster and wider adoption.

The adapted Kitchenham and Charters (2007) assessment revealed significant variation among the eleven included studies. As shown in Table 5, two studies were classified as Low Quality, five as Medium Quality, and four as High Quality. These findings indicate that although several literature reviews are well conducted, the majority exhibit methodological limitations that may affect their reliability. This, in turn, highlights the need for more rigorously designed research on the topics of CC and CCCS.

4.2. Identifying Current Research Gaps in CCCS for Future Research

As previously outlined, uncertainty surrounding the security of CC is a major barrier to its adoption by many organisations. This study identifies eight core literature gaps in CCCS that warrant further investigation. An analysis of these gaps shows that some were highlighted more frequently across the reviewed studies than others.

4.2.1. Further Research on Various Security Issues in CC

One crucial area for future study is the development of a more comprehensive understanding of the diverse security concerns present in the field of CC. CCCR, identified in five of

the eleven publications analysed in this study, poses a significant obstacle to the adoption of CC. Accordingly, future research should prioritise addressing the uncertainties arising from these gaps in order to facilitate a secure transition to cloud services for organisations. Such research must be more rigorous, reproducible and methodologically sound so as to improve its reliability and facilitate CC adoption and CCCS management. Moreover, the findings indicate the need for additional studies addressed at properly managing organisational and human-centred gaps.

4.2.2. Further Development of Cryptographic Algorithms (Such as Genetic and DNA Cryptography) and Their Application to Emerging Technologies

Five out of the eleven studies emphasised the need for further research on cryptographic algorithms and their applications to improve the effectiveness of CC. The use of such algorithms has attracted scholarly attention due to its capacity to encrypt confidential information. The studies by Dawson et al. (2023a), Dawson et al. (2023b), Can et al. (2025), Naseri et al. (2023), and Jha et al. (2023) all acknowledge the importance of advancing cryptographic algorithms—particularly through developments in genetic and DNA cryptography—to enhance the security of cloud-based data.

4.2.3. The Need to Establish Stronger Regulatory Standards and Further Develop Frameworks for Improved Cloud Cybersecurity

Another gap identified for future research is the need to establish more rigorous regulatory standards and frameworks specifically designed to address the security requirements of cloud-based infrastructures. CC is a relatively new and rapidly evolving technology; consequently, many service users have not yet had sufficient time to fully understand and adapt to it, while continuous technological advancements create additional gaps. Through the establishment of cloud-specific regulatory standards (Naseri et al., 2023), as well as operational frameworks for use within cloud-based infrastructures (Komar et al., 2023; Soveizi et al., 2023), a more organised and secure approach to CC adoption can be achieved, potentially on a global scale. Future research should also examine the extent to which the forthcoming DORA regulation may contribute to addressing this issue.

4.2.4. Further Research on the Integration of Emerging Technologies (Such as AI, IoT, CC, and Edge Computing) for Improved Cybersecurity

The current pace of technological development indicates an increasing integration of emerging technologies into organisational operations. This study has identified that this trend is likewise evident in CC. Three papers included in this review indicate the integration of CC with emerging technologies such as AI, IoT, blockchain, quantum computing, and edge computing (Komar et al., 2023; Naseri et al., 2023; Surianarayanan & Chelliah, 2023). As was the case with the introduction of CC as an emerging technology, this convergence brings both solutions to existing security challenges and the need for new safeguards to address emerging vulnerabilities resulting from such technological amalgamations.

4.2.5. Further Developments of Cyber Risk Management Tools to Keep Pace With the Evolution of Cyber Risks

Two papers identified within this study also outline the need for further research on the development of cyber risk management tools capable of remaining effective amid rapidly evolving cyber threats. They emphasise that intrusion detection and threat intelligence

systems should be further advanced to better address the requirements of CC infrastructures and the continuously changing threat landscape. Komar et al. (2023) and Rahaman et al. (2023) likewise underscore the need to develop cyber risk management tools specifically tailored to cloud environments. Accordingly, they aim to address this issue by developing a static analyser that implements a security defence mechanism capable of identifying, detecting, and mitigating potential adversarial attacks (Rahaman et al., 2023).

4.2.6. Improvements to Produce Validated, Reproducible Defence Mechanisms for Cloud-Native and Microservice Architectures

Cloud-native and microservice architectures introduce security challenges that existing defence mechanisms do not adequately address. An analysis of the studies by Rahaman et al. (2023) and Minna and Massacci (2023) indicates that future research should prioritise the development of validated, reproducible defence mechanisms capable of securing the full operational stack of cloud-native and microservice-based systems.

5. THEORETICAL IMPLICATIONS

The comparison of studies in this review reveals a consistent theoretical gap in the conceptual clarity surrounding CC and CCCS. The existing literature lacks a unified framework to address the multidimensional nature of CC risks, particularly in relation to stakeholder roles and regulatory boundaries. This fragmentation limits the field's ability to explain or predict security outcomes in increasingly complex CC systems. It therefore underscores the need for theory-building that integrates technological, organisational, and policy perspectives. Future research should aim to refine existing models and design new constructs that account for lifecycle-wide security, cloud-native and microservice architectures, while better capturing the evolving dynamics of CCCS.

6. PRACTICAL IMPLICATIONS

Building on the theoretical need to demystify CC and CCCS, progress requires coordinated efforts across stakeholders. Organisational service users should prioritise targeted cybersecurity training, adopt best-practice frameworks, and conduct regular audits. Regulators must establish clear, standardised requirements and enforce minimum security baselines. Cloud service providers (CSPs) should likewise enhance their practices by integrating robust security tools and models and by collaborating with academic researchers to test new safeguards and comprehensively strengthen CCCS. A further practical implication is that industry currently operates reactively, with developments in CC evolving faster than relevant academic literature. This misalignment increases operational risk and highlights the need for more proactive, evidence-based security practices.

7. LIMITATIONS AND FUTURE LINES OF RESEARCH

7.1. Study Limitations

While a systematic approach was employed to ensure the validity of this study, no single investigation is without limitations. It is therefore important to acknowledge the constraints affecting this research. This section outlines and discusses the principal limitations encountered.

First, it should be noted that although this research provides an overview of cybersecurity and CC, it only considers their interconnected relationship. As such, this research fails to fully represent these topics independently. Consequently, certain gaps specific to one domain may have been overlooked, despite their potential importance for its future development. Furthermore, one of this study's findings revolved around the interconnectedness of different emerging technologies. This study is limited to CCCS and so, there may be other cybersecurity issues which are mainly relevant to other emerging technologies, but which influence all novel technologies. Given the constraints of this research, such issues would not have been identified.

This study analyses papers retrieved from the Google Scholar and Scopus databases. Consequently, other relevant studies may not have been considered if they were unavailable in these sources. Furthermore, the limitations imposed by the inclusion criteria may have resulted in certain eligible studies being overlooked. These limitations included restricting the analysis to literature published in English and fully accessible in its entirety, either as Open Access or through resources provided by the University of Malta. Additionally, limiting the sample to papers published between January and July 2023 meant that a considerable number of studies that could have provided a deeper understanding of the state of the art in CC and CCCS were excluded.

Another such limitation is that the screening and analyses of the selected studies were conducted by a single reviewer, which increases the risk of subjective interpretation and inconsistent decisions, and which in turn may influence study selection and analysis. While measures were taken to mitigate this limitation, the lack of a second independent reviewer means that some level of bias may still be present.

7.2. Outlined Future Directions

Research gaps for future considerations were outlined by the chosen primary literature papers. These gaps are summarised in Table 3.

Considering Table 4, eight core literature gaps were identified from the included studies. The future requirements derived from these gaps are as follows: (1) further research on cryptographic algorithms and their applications in emerging technologies; (2) greater understanding of CBMSs and their cybersecurity; (3) more clearly established regulatory standards, as well as the development of frameworks to enhance CCCS; (4) additional research on the integration of emerging technologies to strengthen cybersecurity; (5) deeper investigation into the various security issues within CC; (6) further research dedicated to improving the sustainability of CC infrastructures; (7) continued exploration and optimisation of serverless computing; and (8) the development of more effective cybersecurity management tools capable of maintaining relevance amid the rapid evolution of cyber risks.

7.3. Other Gaps To Be Addressed by Future Research

Apart from the eight core literature gaps previously identified in the included studies, additional gaps were also revealed through their analysis and likewise warrant further research. The study highlights a clear need for validated and reproducible defence mechanisms tailored to cloud-native and microservice architectures. Furthermore, several studies point to persistent organisational and human-centred weaknesses that also require dedicated research. The methodological variability observed across the included studies also underscores the need for more rigorous, transparent, and empirically grounded research designs in CCCS, ensuring

that future findings are both reliable and applicable to rapidly evolving cloud environments. Given that cloud technologies continue to evolve faster than the academic literature addressing their security, future research should also focus on accelerating the production of reliable academic literature in such a way that it can keep up with developments in CC, enabling academics and service users to act proactively rather than reactively.

8. CONCLUSIONS

CC is evolving at an extraordinary pace, requiring practitioners and researchers to develop deeper and more adaptive understandings of its technological and cybersecurity implications. This study contributes to the CCCS literature by systematically identifying nine critical research gaps across encryption, system architecture, organisational readiness, and regulatory governance, thereby providing an integrated synthesis of previously fragmented knowledge.

Consistent with recent 2023 literature indicating that digital transformation enhances efficiency while simultaneously intensifying cybersecurity risks and resilience requirements, this study extends prior reviews by offering a structured gap-based perspective that links technological vulnerabilities with organisational and human dimensions. Rather than remaining limited to infrastructure-centric analyses, the findings emphasise the strategic relevance of governance, risk culture, and user awareness as foundational elements of cybersecurity resilience in cloud environments.

The results further underscore the urgency of advancing cyber risk management frameworks, regulatory standards, and cryptographic innovations capable of addressing increasingly complex and adaptive threats. Emerging technological integrations such as AI, the Internet of Things, edge computing, and specialised applications such as CBMSs, introduce new systemic vulnerabilities that demand interdisciplinary and forward-looking research agendas.

From a theoretical standpoint, this study advances beyond descriptive synthesis by consolidating dispersed evidence into a coherent conceptual understanding of CCCS gaps, thereby transforming isolated findings into a structured research agenda. From a practical perspective, it highlights the centrality of organisational preparedness, cybersecurity awareness, and governance maturity as prerequisites for secure digital transformation. Ultimately, strengthening cybersecurity in CC is not solely a technical imperative but also a sociotechnical requirement for protecting digital economies, preserving privacy, and sustaining institutional trust in an increasingly interconnected world.

STATEMENTS

Acknowledgments

This work is primarily based on a thesis by Tristan Barbara, submitted in partial fulfilment of the MSc in Insurance and Risk Management at the University of Malta in 2023, under the supervision of Dr. Christian Bonnici West.

Data Availability

This study is based on a review of existing literature; therefore, no primary data were generated or analyzed.

Use of Artificial Intelligence

The author declares that no AI tools were used for the creation or analysis of the manuscript's content; their use was limited to grammar correction and language refinement.

Conflicts of Interest

The author declares no conflicts of interest.

Funding

This research did not receive any specific funding.

Author Contribution (CRediT)

TB: conceptualization, methodology, formal analysis, writing, original draft, review & editing.

Ethical Approval

Ethical approval was not required.

Originality Statement

The author declares that this manuscript is original, has not been previously published, and is not under consideration for publication elsewhere. This article is based on a prior master's thesis.

REFERENCES

Amazon Web Services, Inc. (n.d.). *What is cloud computing?* Amazon Web Services. https://aws.amazon.com/what-is-cloud-computing/

Bennasar, H., Bendahmane, A., & Essaaidi, M. (2017). An overview of the state-of-the-art of cloud computing cyber-security. In S. El Hajji, A. Nitaj, & E. Souidi (Eds.), *Lecture notes in computer science: Vol. 10194. Codes, cryptology and information security* (pp. 56–67). Springer. https://doi.org/10.1007/978-3-319-55589-8_4

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the ACM Conference on Computer and Communications Security, Raleigh, NC, USA*, 833–844. https://doi.org/10.1145/2382196.2382284

Can, O., Thabit, F., Aljahdali, A. O., Al-Homdy, S., & Alkhzaimi, H. A. (2025). A comprehensive literature of genetics cryptographic algorithms for data security in cloud computing. *Cybernetics and Systems, 56*(5), 413–447. https://doi.org/10.1080/01969722.2023.2175117

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21. https://doi.org/10.22215/timreview/835

Dawson, J. K., Twum, F., Hayfron Acquah, J. B., & Missah, Y. M. (2023a). Reconnoitering security algorithms performance in the cloud: Systematic literature review based on the PRISMA

archetype. *Journal of Theoretical and Applied Information Technology, 101*(6), 2203–2227. http://www.jatit.org/volumes/Vol101No6/14Vol101No6.pdf

Dawson, J. K., Twum, F., Hayfron Acquah, J. B., & Missah, Y. M. (2023b). PRISMA archetype-based systematic literature review of security algorithms in the cloud. *Security and Communication Networks, 2023*(1), Article 9210803. https://doi.org/10.1155/2023/9210803

Douglis, F., & Nieh, J. (2019). Microservices and containers. *IEEE Internet Computing, 23*(6), 5–6. https://doi.org/10.1109/MIC.2019.2955784

Ganne, A. (2022). Emerging business trends in cloud computing. *International Research Journal of Modernization in Engineering Technology and Science, 4*(12), 459–462. https://doi.org/10.56726/irjmets32082

Hernandez, A. (2022). *What are the emerging and future technologies that we will have to worry the most about from a security perspective?* [Course paper]. Old Dominion University. https://sites.wp.odu.edu/aaronhernandez/wp-content/uploads/sites/17871/2023/04/CYSE-426-Project-Paper.pdf

Institute of Risk Management. (2014). *Cyber risk: Resources for practitioners* [White paper]. Institute of Risk Management. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

Jha, R., Kumari, N., & Omeribe, C. C. (2023). Cloud privacy and security- A review paper. *Vidhyayana, 8*(7), 333–351. https://www.vidhyayanaejournal.org/journal/article/view/828

Khan, S., Khan, S., & Galibeen, S. (2011). Cloud computing an emerging technology: Changing ways of libraries collaboration. *International Research: Journal of Library and Information Science, 1*(2), 151–159. https://www.proquest.com/docview/1267541922

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE Technical Report EBSE-2007-01). Software Engineering Group, School of Computer Science and Mathematics, Keele University & Department of Computer Science, University of Durham.

Komar, R., Patil, A., & Ali, W. A. (2023). Emerging trends in cloud computing: A comprehensive analysis of deployment models and service models for scalability, flexibility, and security enhancements. *Journal of Intelligent Systems and Applied Data Science, 1*(1), 20–28. https://jisads.com/index.php/1/article/view/10/5

Li, Y., Lin, Y., Wang, Y., Ye, K., & Xu, C. (2023). Serverless computing: State-of-the-art, challenges and opportunities. *IEEE Transactions on Services Computing, 16*(2), 1522–1539. https://doi.org/10.1109/TSC.2022.3166553

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800145). U.S. Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Microsoft. (n.d.). *What is cloud computing?* Azure. https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

Minna, F., & Massacci, F. (2023). SoK: Runtime security for cloud microservices. Are we there yet? *Computers & Security, 127*, Article 103119. https://doi.org/10.1016/j.cose.2023.103119

Naseri, F., Kazemi, Z., Larsen, P. G., Arefi, M. M., & Schaltz, E. (2023). Cyberphysical cloud battery management systems: Review of security aspects. *Batteries, 9*(7), 382. https://doi.org/10.3390/batteries9070382

National Institute of Standards and Technology. (n.d.). Cybersecurity. In *NIST glossary*. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity

Nightingale, A. (2009). A guide to systematic literature reviews. *Surgery (Oxford), 27*(9), 381–384. https://doi.org/10.1016/j.mpsur.2009.07.005

Nobanee, H., Alodat, A., Bajodah, R., AlAli, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime, 30*(6), 1736–1754. https://doi.org/10.1108/JFC-11-2022-0287

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., MayoWilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *British Medical Journal, 372(71)*, 1–9. https://doi.org/10.1136/bmj.n71

Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2023). The survey and metaanalysis of the attacks, transgressions, countermeasures and security aspects common to Cloud, Edge and IoT. *Neurocomputing, 551*(C), Article 126533. https://doi.org/10.1016/j.neucom.2023.126533

Rahaman, M. S., Islam, A., Cerny, T., & Hutton, S. (2023). Staticanalysisbased solutions to security challenges in CloudNative systems: Systematic mapping study. *Sensors, 23*(4), Article 1755. https://doi.org/10.3390/s23041755

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology? *Research Policy, 44*(10), 1827–1843. https://doi.org/10.1016/j.respol.2015.06.006

Soveizi, N., Turkmen, F., & Karastoyanova, D. (2023). Security and privacy concerns in cloudbased scientific and business workflows: A systematic review. *Future Generation Computer Systems, 148*, 184–200. https://doi.org/10.1016/j.future.2023.05.015

Spelman, R. (2015, October 26). *The definition of cloud computing*. Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2015/10/26/the-definition-of-cloud-computing/

Surianarayanan, C., & Chelliah, P. R. (2023). Integration of the Internet of Things and Cloud: Security challenges and solutions – A review. *International Journal of Cloud Applications and Computing, 13*(1), 1–30. https://doi.org/10.4018/ijcac.325624

Susnjara, S., & Smalley, I. (n.d.). *What is cloud computing?* IBM. https://www.ibm.com/topics/cloud-computing/

Xu, D. (2010). Cloud computing: An emerging technology. *Proceedings of the 2010 International Conference on Computer Design and Applications (ICCDA 2010), Qinhuangdao, China,* 37–40. https://doi.org/10.1109/ICCDA.2010.5541105