Assessing future development needs in cloud computing cyber security: A systematic literature review of literature reviews

Tristan Barbara

A dissertation submitted in partial fulfilment of the requirements of the Masters of Science in Insurance and Risk Management at the University of Malta

September 2023

Abstract:

Cloud computing is an innovative technology which presents significant changes to the way organisations and individuals satisfy their computing needs. However, the rapid growth of emerging technologies, including cloud computing, creates significant cybersecurity gaps and issues for service users. These gaps, paired with the increasing popularity of the cloud, warrant the need for further research to be done for improving this technology and ensuring its safety and reliability. This thesis presents a systematic literature review of other literature reviews published on the Google Scholar and Scopus databases, with the aim of outlining the main gaps that require future research on this topic. Furthermore, this study analyses the included literature to assess the extent to which studies address the awareness, or lack thereof, of business organisations and their employees on the importance of cyber security in their uses of cloud computing. Through the inclusion and exclusion criteria set, a total of eleven studies were identified and analysed to the extent of addressing this research's aims. The results obtained show that there are numerous research gaps of various natures, which require further research. It was also outlined how these research gaps must be addressed for cloud computing to become a safer and more reliable technology for organisations.

Acknowledgements

I would like to take this opportunity to thank my dear family and friends for their continuous support and sacrifice in helping me to complete this thesis. I would also like to thank my tutor, Dr Christian Bonnici West, for his continued assistance and guidance. Finally, I would like to thank the University of Malta's Department of Insurance and Risk Management for their support throughout my Masters of Science in Insurance and Risk Management course.

Table of Contents

Abstract: ii

Acknowledgements iii

Table of Contents iv

List of Tables vii

List of Figures viii

Chapter 0. Preliminary Information ix

Chapter 1. Introduction 1

1.1. Background 1

1.2. Research problem and aims 3

1.3. Exploratory and Research questions 4

1.3.1. Exploratory Questions 4

1.3.2. Research Questions 5

1.4. Research Significance 5

1.5. Thesis Structure 6

Chapter 2. Preliminary Literature Review 9

2.1. Exploratory Questions 9

2.2. EQ1: What is cloud computing? 10

2.2. EQ2: What is cyber security? 12

2.3. EQ3: How are cyber security and cloud computing related? 14

2.4. The construction of RQ1: 15

2.5. The most common forms of cloud computing cyber security risks 16

2.6. The role of cyber security in organisational resilience 18

2.7. The construction of RQ2: 19

2.8. The concurrent legislation and regulation at EU level that govern cyber security. 20

Chapter 3. Methodology 23

3.1. Determining the exploratory questions 23

3.2. Research strategy and criteria 24

3.3. Screening process 30

3.4. Data extraction process 30

3.5. Assessing risk of bias in the included research studies 31

3.6. Data synthesis methodology 31

3.7. Measures for avoiding bias in the data collection and analysis phases 32

Chapter 4. Results 33

4.1. Selection of Primary Literature 33

4.2. Analysis of results 35

4.2.1. Cryptographic algorithms for the encryption of cloud data 38

4.2.2. Cloud-based Workflow Management Systems 40

4.2.3. Cloud Battery Management Systems (CBMS) 42

4.2.4. Challenges faced by organisations in their adoption and use of cloud computing . 44

4.2.5. Existing defensive solutions and tools for improving the security of microservice architectures and cloud-native systems 46

4.2.6. The integration of cloud computing systems with emerging technologies 47

4.3. Outlined future directions 50

Chapter 5. Discussion 54

5.1. Analysis of the findings 54

5.2. Identifying concurrent research gaps in cloud computing cyber security that should be addressed by future research 55

5.2.1. Further research on various security issues in cloud computing. 55

5.2.2. Further development of cryptographic algorithms (such as Genetic and DNA cryptography) and their application to emerging technologies. 56

5.2.3. The need for the establishment of better regulatory standards and further developments of frameworks to be followed for better cyber security within the cloud. ... 56

5.2.4. Further research on the integration of emerging technologies (such as AI, IoT, Cloud Computing, and Edge Computing) for better cyber security. 57

5.2.5. Further developments on cyber risk management tools to keep up with the evolution of cyber risks. 57

5.2.6. Other gaps recommended to be addressed by future research. 58

5.3. To what extent do review articles address the awareness, or lack of awareness, of employees on cloud computing cyber security? 59

6. Conclusions 61

6.1. Limitations of this study 61

6.2. Concluding Remarks and Recommendations for Future Investigations 62

References 64

List of Tables

Table 3.1: Table of Inclusion and Exclusion Criteria and their justification. 25

Table 4.1.: Table of topics discussed by each identified study (showing the first 6 studies) 36

Table 4.2.: Table of topics discussed by each identified study (showing the remaining 5 studies) 37

Table 4.3.: Table of identified future recommendations for each identified study (showing the first 5 studies) 51

Table 4.4.: Table of identified future recommendations for each identified study (showing the remaining 5 studies) 52

List of Figures

Figure 1.1: Schematic Research Methodology Diagram 8

Figure 4.1: Flow Diagram depicting the screening process of the identified studies 34

Chapter 0. Preliminary Information

This section is organised in 14 sections, each defining a key term used in this thesis.

0.1 Cloud Computing

The definition adopted for ‘cloud computing’, based on a definition proposed by Microsoft (2023), is as follows:

> **Definition 1 (cloud computing):** *“The delivery of computing services over the Internet.”* (Microsoft, 2023)

0.2 Cyber security

The definition adopted for ‘cyber security’ based on the definition proposed by the National Institute of Standards and Technology (NIST) (2023), is as follows:

> **Definition 2 (cyber security):** *“Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”* (NIST Computer Security Resource Centre, 2023)

0.3 Service Provider

The definition adopted for ‘service provider’, based on the definition proposed by Google Cloud (2023), is as follows:

Definition 3 (service provider): *"A cloud service provider, or CSP, is an IT company that provides on-demand, scalable computing resources like computing power, data storage, or applications over the internet" (Google Cloud 2023).*

0.4 Service User

The definition adopted for 'service user' is as follows:

Definition 4 (service user): *"A legal or natural person that uses the cloud-based products offered by a service provider."*

0.5 Cloud Computing Cyber Security

The definition adopted for 'cloud computing cyber security' is as follows:

Definition 5 (cloud computing cyber security): *"The cyber security of cloud computing processes and systems."*

0.6 Emerging Technology

Over the years, numerous articles were written on the definition and effects of emerging technologies, which have become a subject of increasing discussion among academics. Modern technology's rapid development is the primary cause of this. The following is the definition adopted for 'emerging technology' in this thesis, which is based on the definition proposed by Rotolo, Hicks, et al. (2015). As such, this definition emphasises the importance of five criteria; i.e.: (i) radical novelty, (ii) relatively fast growth, (iii) coherence, (iv) prominent impact, and (v) uncertainty and ambiguity:

Definition 6 (emerging technology): *"A radically novel and relatively fast-growing technology characterised by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domain(s) which is observed in terms of the composition of actors, institutions and patterns of interactions among those, along with the associated knowledge production processes" (Rotolo, Hicks et al. 2015).*

0.7 Artificial Intelligence

The definition adopted for 'Artificial Intelligence' (or AI) is as follows, based on (European Parliament 2023):

Definition 7 (AI): *"(T)he ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity" (European Parliament 2023).*

0.8 Internet of Things

The definition adopted for 'Internet of Things' (or IoT) is as follows, based on (The International Business Machines Corporation (IBM) (2023)):

Definition 8 (IoT): *"A network of physical devices, vehicles, appliances and other physical objects that are embedded with sensors, software and network connectivity that allows them to collect and share data." (The International Business Machines Corporation (IBM) 2023)*

0.9 Zero-day vulnerability, zero-day exploit, and zero-day attack

The following definitions adopted for ‘zero-day vulnerability’, zero-day exploit’, and ‘zero-day attack’ are as follows, based on Kaspersky (2023):

Definition 9 (zero-day vulnerability): *“a software vulnerability discovered by attackers before the vendor has become aware of it” (Kaspersky 2023).*

Definition 10 (zero-day exploit): *“the method hackers use to attack systems with a previously unidentified vulnerability” (Kaspersky 2023).*

Definition 11 (zero-day attack): ***“****The use of a zero-day exploit to cause damage to, or steal data from a system affected by a vulnerability” (Kaspersky 2023).*

0.10 Primary literature

The definition adopted for ‘primary literature’ is as follows:

Definition 12 (primary literature): ***“****The studies which were assessed and discussed within this research, following the preliminary screening process in line with the set inclusion and exclusion criteria.”*

0.11 Container

The definition adopted for ‘container’ is as follows, based on the definition provided by Avi Networks (2023):

Definition 13 (container): ***“****Efficient and standard media for applications to move between environments and run independently, containing all that is required for the application to run with the exception of the shared operating system on the server” (Avi Networks 2023).*

0.12 Microservice

The definition adopted for ‘Microservices’, as a core component of cloud-native computing (Tozzi 2022), is as follows, based on Avi Networks (2023):

> **Definition 14 (microservice):** ***“****An architectural design which allows for the building of a distributed application through independent, loosely-coupled, individually deployable services. It allows for the scalability of the individual components of an application, without the disruption of the other components” (Avi Networks 2023).*

0.13 Runtime security

The definition adopted for ‘Runtime security’, is as follows, based on Amazon Web Services (2023):

> **Definition 15 (runtime security):** ***“****An architecture which provides active protection for containers while they're running” (Amazon Web Services 2023).*

0.14 Serverless computing and backend services

The definitions for ‘serverless computing’ and ‘backend services’, are as follows, based on Cloudflare (2023):

> **Definition 16 (serverless computing):** *“Serverless computing is a method of providing backend services on an as-used basis” (Cloudflare 2023). “Serverless computing allows developers to purchase backend services on a flexible ‘pay-as-you-go’ basis, meaning that developers only have to pay for the services they use” (Cloudflare 2023).*

Definition 17 (backend services): *“The backend is the part (of the application) that the user doesn’t see; this includes the server where the application's files live and the database where user data and business logic is persisted” (Cloudflare 2023).*

Chapter 1. Introduction

This introductory chapter is organised as follows. In section 1.1, the research background and context are presented. In section 1.2 an outline is provided of the research problem, aims and objectives. In section 1.3, the exploratory and research questions are presented. In section 1.4, the significance of the research is discussed. Finally, in section 1.5, an outline is provided of the remaining parts of this thesis.

1.1. Background

Today's ever increasing technological advances are leading to a technological dependency unlike ever before. Such developments have revolutionised the world as we know it, leading to firms of all sizes implementing increasingly innovative technologies within their organisational processes. The most disrupting and game-changing technologies found in contemporary times are known as emerging technologies. These technologies stem from ground breaking innovations that have brought drastically new solutions to the problems of the modern era. They include technologies like Artificial Intelligence (AI), Cloud Computing (CC), the Internet of Things (IoT), and the Blockchain. However, these examples only scratch the surface of the deep ocean that are Emerging Technologies.

This increased use of, and dependency on technology, as well as the novel changes brought about by these emerging technologies, have provided significantly better solutions to the everyday operational challenges faced by organisations. However, innovation also brings with it a certain degree of uncertainty and, thus, risk. Such risks must be managed, and cybersecurity is an essential tool in this regard. The EU parliament remarks on this issue, emphasising the need to develop a more coherent EU-wide cybersecurity mindset for managing the increasing

number of cyber-attacks, and the incurred costs that organisations are facing on a global level. (European Parliament 2023)

In 2023, Hamed Taherdoost reviewed and summarised the main points of a total of 98 academic papers and provided a very comprehensive overview of the many changes, both positive and negative, that Emerging Technologies are causing on information systems world-wide (Taherdoost, 2023). His conclusions remarked on the works done through his 2021 paper, wherein it was determined that, apart from the effects brought about an organisation's internal operations, an organisation must also consider the consumers' levels of "acceptance and engagement" (Taherdoost, 2021) in successfully implementing a new technology.

Cloud computing, being one such revolutionary technology, has reformed the computing operations of industries world-wide. It is a digital tool which enables service providers to offer customers "on-demand access" "to computing resources" remotely through the internet (The International Business Machines Corporation (IBM), 2023). Such a technology has brought about significant changes since its introduction, radically changing the ways by which organisations and individuals seek to address their computing needs. Concerning the management of hardware and software, cyber security is a process that regards the protection of electronic systems and digital resources from cyber risks. Considering the increasingly technology-dependent world we live in, cyber security is becoming increasingly important for the efficient operations of organisations, as well as an essential factor for their resilience. In understanding the nature of cloud computing and cyber security, it can clearly be seen how these two topics are closely related.

1.2. Research problem and aims

By looking at currently available academic literature, it can be noted that there are numerous works addressing cloud computing, cyber security, and their links. In such literature, it is evident that cloud computing and cyber security are complex topics that evolve in unpredictable ways. Furthermore, these two topics have an impactful effect on the world's economies and the general public's well-being. This complexity is accentuated when combining the two topics together and analysing the cyber security of cloud computing systems. Given their high impact and unpredictability, it is essential that adequate research is conducted to allow for industry professionals and regulators to keep up with this rapidly developing industry. In their review article, Rabai, Jouini et al. (2017) had examined the most recent updates and developments of cloud computing cyber-security at the time. They had concluded that cloud computing is maturing at a very promising rate, further adding that there are "many research directions still open and which promise continued improvements of cloud security and privacy." (Rabai, Jouini et al. 2013). Various publications were viewed to identify current research trends on the subject of cloud computing cyber security. In their study on the evolving cyber security threats, Mijwil, Unogwu et al. (2023) conclude their research by noting the complex and ever-changing nature of cybersecurity risks. In their conclusions, they refer to the use of Artificial Intelligence (AI) as the "preferable" means of mitigating the ever-changing cybersecurity risks of the present (Mijwil, Unogwu et al. 2023). Extending this train of thought, Kaur, Gabrijelčič et al. (2023) conducted a systematic literature review study, in which they examined the various uses of AI in the field of cyber security. They also outlined a number of literature gaps concerning this topic, one of which regarded the mitigation of zero-day attacks. In this specific observation, the authors comment on the importance of having "complete visibility across the entire information technology environment, including endpoints, networks and cloud" (Kaur, Gabrijelčič et al. 2023). Therefore, the research problem being addressed by this study is the rapid and unpredictable evolution of the worlds of cloud computing and cyber security which are creating new and unforeseen challenges to industry professionals and academics alike.

This research aims to address this problem by delving into the vast oceans of cyber security, cloud computing and their interconnected relationship. Through a systematic literature review, this research analyses the concurrent issues as identified within the literature, and identifies what such literature says in relation to the future of cloud computing cyber security. The objective of conducting this systematic literature review is to develop a systematic and methodological research study through which identifies the main gaps and expected future developments within the cloud computing cyber security industry. This study aims to contribute to further enhancing this visibility by creating a comprehensive review on the various literature gaps surrounding cloud computing cyber security as well as the lack of awareness of cloud users on the importance of their organisations' cloud computing cyber security. Further to this, the objective of this study is to provide guidance to future studies on the various research gaps and future research directions of cloud computing cyber security.

1.3. Exploratory and Research questions

This section presents the exploratory questions (EQs 1 to 6), which were used to guide this study's preliminary literature review, which provided the necessary insight for understanding the nature of cloud computing cyber security. It also presents the research questions (i.e., RQs 1 and 2), which build on EQs 1 to 6, insofar as they emerged from the preliminary literature review.

1.3.1. Exploratory Questions

The following are EQs 1 to 6:

EQ1: What is cloud computing?

EQ2: What is cyber security?

EQ3: How are cyber security and cloud computing related?

EQ4: What are the most common cloud computing cyber security risks for business organisations?

EQ5: Why is cyber security important for the survivability of businesses?

EQ6: How are EU regulators currently addressing cloud computing cyber security within member states?

1.3.2. Research Questions

The following research questions stemmed from the preliminary literature review and have driven and guided this systematic literature review:

RQ1: What research gaps in cloud computing cyber security are identified by state-of-the-art literature review articles?

RQ2: To what extent do review articles address the awareness, or lack thereof, of employees on cloud computing cyber security?

1.4. Research Significance

An organisation's survivability depends on how detailed and granular their risk management framework is. Thus, it is imperative that organisations are properly equipped with the necessary knowledge and tools to manage their risks, and to ensure the survivability of their business. This is more so considering the continuously evolving and unprecedented natures of digital emerging technologies such as Cloud Computing (CC). Cyber security is one such practice which organisations employ for the management of their cyber risks. When considering the digital

nature of cloud computing, it can clearly be seen how cyber security can be considered one of the most appropriate risk management practices for such a technology.

With organisations globally reaching for more digitalised operations, cyber security has become ever more essential for the effective adoption and use of the various technologies made available to these organisations. Such an importance on cyber security, paired with the constantly evolving nature of cloud computing means that further research is constantly required on these topics. This is important for current industry professionals who make use of these tools, as it will provide better oversight on these two subjects and their inter-related developments. This research would thus be significant as a reference point for academics and organisations alike in that it provides a concurrent overview of the gaps in cloud computing cyber security, as well as the future directions of these two topics. This would also provide guidance on what studies should be made in the future.

1.5. Thesis Structure

This thesis is structured as follows: In Chapter 1, an outline of the study and the motivation behind it is provided. Here, the research aims are explained, and the exploratory and research questions which were used to guide this study are outlined briefly. Furthermore, an outline of the structure of the remaining chapters is also provided. Chapter 2 presents a Preliminary Literature Review. Here, the exploratory questions set in Chapter 1 were followed for the construction of a background on the topic of cloud computing cyber security. Through this chapter, the research questions are also constructed as a product of the findings made by the preliminary literature review. In Chapter 3, the methodology employed for conducting this research study is explained in detail. Within Chapter 4, the results obtained in following the methodology set in chapter 3 are outlined. In Chapter 5, a discussion on the results outlined is given. Finally, Chapter 6 provides

a conclusion to this research by summarising the findings and providing suggestions for future research.

The structure of the thesis was developed in line with the Schematic Research Methodology Diagram (see Figure 1.1) which was followed in conducting this research, as well as in accordance with the PRISMA checklist. The Schematic Research Methodology Diagram describes the process followed throughout this study.

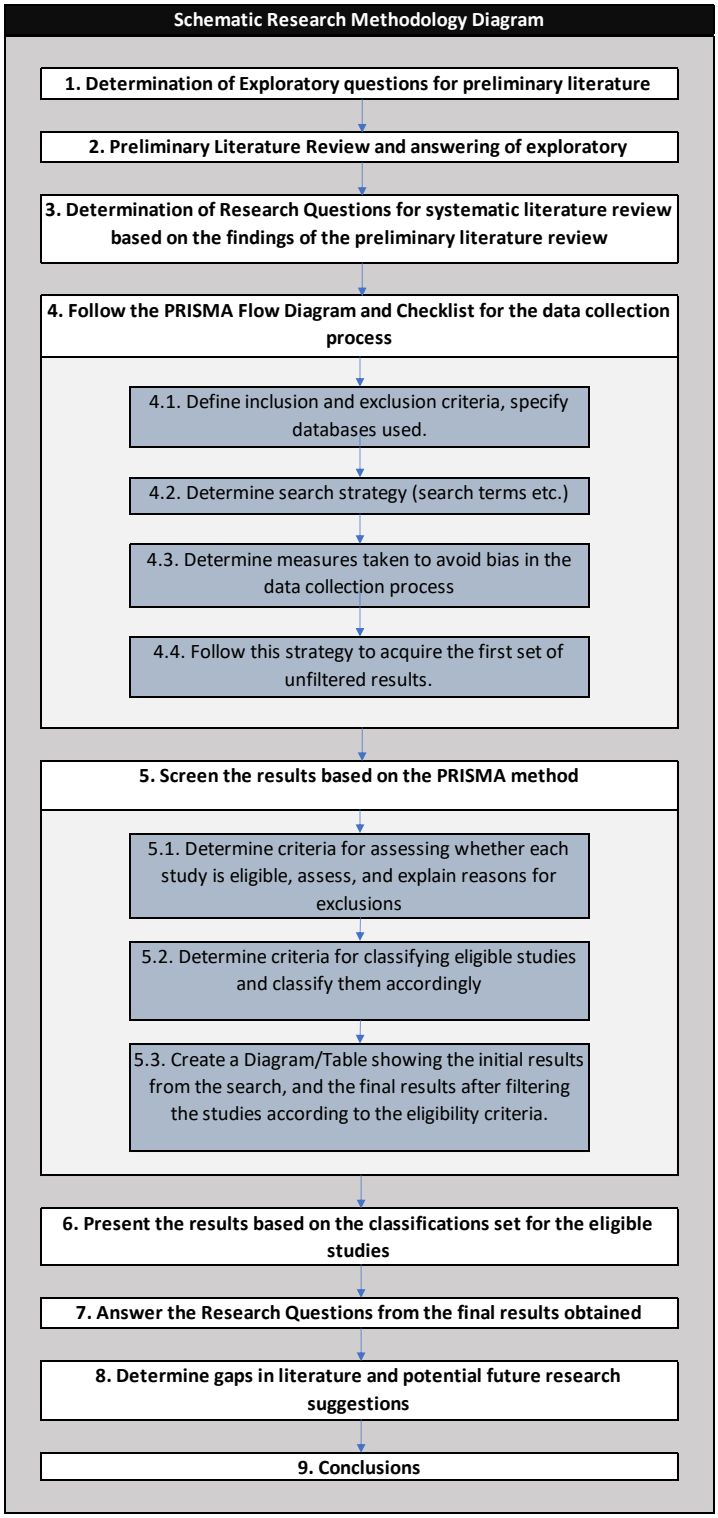

Figure 1.1: Schematic Research Methodology Diagram

Chapter 2. Preliminary Literature Review

This chapter presents a preliminary review of the academic literature related to cloud computing and cyber security, with the aim of providing a brief background on these subjects and to support the preparation and development of this research, by setting a stable foundation on the discussions made in concurrent literature.

In section 2.1, EQs 1 to 6 are explained further. These exploratory questions guide the study and the reader to the development of this study's research questions. Section 2.2 addresses the first three exploratory questions of this study; EQ1, EQ2, and EQ3. This provides an introduction to cyber security and cloud computing by defining and providing a brief overview of the two topics and the relevant discussions made by current literature on the two topics. Furthermore, an overview of the inter-related nature of the two topics is provided. Through this process, the first research question of the study; RQ1, was developed. In section 2.3, the role of cyber security in organisational resilience in light of the various cloud computing cyber security risks is explored. This section addresses exploratory questions EQ4 and EQ5, and leads to the development of research question RQ2. Guided by exploratory question EQ6, Section 2.4 addresses the regulatory aspects of cloud computing cyber security within the context of the EU and its member states. Within this section, the third research question; RQ3, was developed.

2.1. Exploratory Questions

EQs 1 to 6 were used as a guide for this study's preliminary literature review. This allowed for a structured methodology where the exploratory questions guided the preliminary literature review, which in turn led to the development of this study's research questions.

Answers to EQs 1 to 5 provide this study with the necessary background information on cyber security and cloud computing. Such information enabled further probing into the relationship between cloud computing and cyber security through the generation of this study's Research Questions. EQ6 provided insight into the current state of cyber security legislation and regulation within the EU. When considering that cloud computing and cyber security are inter-related, such an exploratory question would portray this relationship from the legal and regulatory aspects. This identifies which regulations should be analysed for determining how current EU regulation and legislation aims to mitigate cloud computing cybersecurity risks and threats in the future.

2.2. EQ1: What is cloud computing?

Cloud computing is a novel and fast-growing technology which has left a significant impact on the world through its revolutionary means of providing users with access to the necessary hardware to conduct their computing organisational activities through the internet. Within literature, one can find a satisfactory level of coherence in both the definition of cloud computing, such as those of The National Institute of Standards and Technology (Mell, Grance, 2011), Amazon Web Service (Amazon Web Services, 2023), Cloud Security Alliance (CSA, 2023), and The International Business Machines Corporation (IBM, 2023), as well as in the consideration of cloud computing being an Emerging Technology, being described as such in a number of literature including by Xu Dong in the 2010 International Conference Proceeding On Computer Design And Applications (Xu, 2010), by Khan Shazia et al. (Khan, Khan et al. 2011), Ganne A. (Ganne, 2022), and by Hernandez Aaron et al. (Hernandez, Karahan, 2022), amongst others. This classification is a fundamental aspect of this study as by being an emerging technology, cloud computing is inherently a revolutionary technology which has brought about significant changes to the way organisations and individuals approach certain tasks.

Further enhancing this technology's coherence amongst academics and industry professionals alike, the definition of cloud computing can be acquired from a number of different sources. The International Business Machines Corporation (IBM) defines cloud computing as *"on-demand access, via the internet, to computing resources" "hosted at a remote data center managed by a cloud services provider"* (IBM, 2023). Typically made available as a subscription-based service or billed based on usage (IBM, 2023), this revolutionary technology can be scaled up or down depending on the user's needs (Cloud Security Alliance (CSA), 2023), and is a cost-effective alternative to *"buying, owning, and maintaining physical data centers and servers"* (Amazon Web Services, 2023) through its "On-demand self-service" (Mell, Grance, 2011). Similarly, Microsoft defines Cloud Computing as "the delivery of computing services" "over the Internet" (Microsoft, 2023). Such a system enables users to only pay for computing services that they use, allowing them to benefit from lower costs and more efficient operations. Additionally, cloud computing allows users to vary their usage of different computing services based on their needs, further increasing efficiency. Cloud computing is a general term which encompasses a number of variations. Microsoft subdivides cloud computing into four main categories: "Infrastructure as a Service (IaaS)", "Platform as a Service (PaaS)", "Software as a Service (SaaS)", and "Serverless Computing". Although these types may differ from one another, they all revolve around the core concept of a service provider who typically has ownership of a computing-based product or service, and who allows other entities to use this product or service remotely, through the internet, in exchange for payment. Real world examples of such products include email platforms such as Outlook, cloud storage products like Google Drive, and several others like Amazon Web Service and Dropbox. Furthermore, cloud computing sees its use in a number of varying industries such as the medical industry (Vellela, Reddy et al. 2023), and governmental institutions (Kumar, Kathuria et al. 2023)

Cloud computing is a malleable technology in that there are multiple ways through which is can be offered and used. As such, cloud computing is commonly classified by one of four deployment models; Private cloud, public cloud, hybrid cloud, and community cloud (Komar, Patil 2023). Private cloud models refer to cloud infrastructures which are specifically intended for the use of a singular organisation. On the contrary, public cloud models provide a system of “shared infrastructure and services” (Komar, Patil 2023). The Hybrid cloud model refers to a combination of both the private and the public cloud models, whereas the Community cloud model refers to a cloud computing service and infrastructure which is shared among organisations “with common interests” (Komar, Patil 2023).

Cloud computing’s history is a relatively short one, seeing the first instance of commerciality in 1977 through the Chase Manhattan Bank’s (New York) Local Area Network (LAN) (Can, Thabit et al. 2023). Can, Thabit et al. (2023) outline further developments from this instance, notably the creation of the World Wide Web in 1989, the founding of the service provider; Sales Force, in 1999, Amazon Web Services’ initial supply of IaaS cloud computing service, the introduction of Docker’s open-source container software in 2013, and leading to 2020, where the authors note the role of Edge computing in reforming the way cloud computing “is used in critical economic areas” (Can, Thabit et al. 2023). Through the work of Can, Thabit et al. (2023), we see the drastic developments of cloud computing, from an initial LAN in 1977, to a technology which was expected to have datacentre speeds of over 1,000 G by 2021 (Can, Thabit et al. 2023), and all of this in less than 45 years.

2.2. EQ2: What is cyber security?

Today’s ever increasing technological advances are leading to a dependency on technology unlike ever before. These technological advances have revolutionised the world as we know it,

leading to firms of all sizes implementing more advanced technologies within their organisational processes. Such an example would be the increasing use of cloud-based systems. Such an increased use and dependency on technology has left businesses needing to more effectively manage their cybersecurity risks. The Institute of Risk Management defines Cyber Risk as “any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems” (The Institute of Risk Management, 2014). When analysing this definition, cybersecurity risk could thus be defined as the risk of loss originating from a failure in the use of information technology systems. Through the above definition of cybersecurity risk, one can thus define cyber security. Much like its risks, cyber security is a very general term which may be interpreted in a multitude of ways by different academics and industry professionals. In considering this, Craigen Dan et al. had conducted a research project in 2014 with the aim of finding an appropriate definition, capable of unifying other interpretative definitions into one common understanding of cyber security (Craigen, Diakun-Thibault et al. 2014). Through their research, Craigen et al. defined cyber security as: “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." (Craigen, Diakun-Thibault et al. 2014). They further explain how this definition captures the complexity of cyber security, the multitude of risks attributable to it, as well as the various views presented on the “ownership and control” of digital assets. (Craigen, Diakun-Thibault et al. 2014). The National Institute of Standards and Technology (NIST) define cyber security as the “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” (NIST Computer Security Resource Centre, 2023). When comparing the definition of NIST with that of Craigen et al., some differences can be identified yet, it can be seen that although almost a decade apart, both definitions regard the protection of electronic systems and digital resources.

This defines cyber security and thus, answers this study's second exploratory question '**EQ2:** What is cyber security?'

2.3. EQ3: How are cyber security and cloud computing related?

In view of the above definitions, we proceed to answering the third exploratory question; '**EQ3:** How are cyber security and cloud computing related?'. Cloud computing refers to internet-based systems where computer services are offered remotely. The inherently digital nature of both cloud computing and cyber security directly implies their inter-relation. Cloud Computing's radical novelty gave way for a considerable degree of change in the world as we knew it by changing the way we look at computing products and services. The revolutionary shift, from computing facilities being limited by their physical nature, to the ability to access computing services remotely through the internet has truly reformed the way computing services are looked at by both individuals and companies alike. This new approach to computing has created opportunities for more effective operations at lower costs, enabling the technological and computing industry to reach greater lengths than ever before. Unfortunately, where innovation goes, new risks follow suit, and cloud computing is no exception. In fact, Mijwil, Unogwu et al., (2023) identifies cloud computing as one of "the Top Five Evolving Threats in Cybersecurity" (Mijwil, Unogwu et al., 2023). They discuss how the simplified solution that cloud computing provides to computing services, paired with improper "encryption and authentication" and "configuration of cloud settings", are the main motivators of cyber security risks (Mijwil, Unogwu et al. 2023). The paper written by Saeed, Altamimi et al. (2023) further emphasises this. In their paper, the authors clearly identify the relationship between cloud computing and cyber security, stating that cloud computing, together with other emerging technologies, are creating more cybersecurity risks to organisations which implement these technologies into their operations (Saeed, Altamimi et al. 2023). Whilst cloud computing can be seen to have negative effects on cyber security, it also presents new opportunities for more effective cybersecurity techniques, frameworks, and programs. The study made by Guo, Guo (2023) found that the cloud-based

algorithm for virus detection and defence had “much higher” success rates “than that of the traditional method” (Guo, Guo 2023). The 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) outlined both the positive and negative effects of cloud computing on cyber security. In this conference proceeding, the authors highlight how, although the increased accessibility of data within cloud computing systems presents new cyber security and information security risks, “cloud computing also provides different services to protect against” such risks (Hasan, Hussain et al. 2023).

2.4. The construction of RQ1:

While the previously mentioned literature was effective in understanding the nature of cyber security and cloud computing, a gap was identified within such literature. It was noted that only select studies address the current and future gaps present on the topic of cloud computing cyber security. Having said that, there is literature, such as the bibliometric analysis conducted by Nobanee, Alodat et al. (2023), that highlights the gaps in literature on “the assessment of cybersecurity risks in emerging technologies” (Nobanee, Alodat et al. 2023). Considering such gaps, this study’s first research question was developed:

RQ1: What research gaps in cloud computing cyber security are identified by state-of-the-art literature review articles?

In answering this research question, this research would provide better insight on the which topics require further studies and analyses by academics. Furthermore, the identification of such gaps would help guide future research in a manner which better demystifies the world of cloud computing cyber security.

2.5. The most common forms of cloud computing cyber security risks

The ever-evolving nature of the internet and digitalisation has led to the creation of numerous emergent risks for companies and individuals alike. In their review article, Mijwil, Unogwu et al. (2023) identify “Ransomware Attack”, “IoT Attacks”, “Cloud Attacks”, “Phishing Attacks”, and “Cryptocurrency and Blockchain Attacks” as the five most common and influential forms of cyber threats in contemporary times (Mijwil, Unogwu et al. 2023). In their paper, Mijwil, Unogwu et al. (2023) also reference two papers, that of Shafiq, Gu et al. (2022), and that of Kimani, Oduol et al. (2019). In both papers, the authors make specific reference to the various types of Internet of Things (IOT)-based cybersecurity threats. The paper written by Aslan, Aktuğ et al. (2023) provides a very comprehensive overview of the nature of cyber security, namely the numerous forms of related threats, vulnerabilities, and attacks present in current times. They discuss these various digital perils in detail, and also provide a considerable degree of suggestions on possible techniques which organisations can employ in their efforts to manage the effects caused by these ever-changing risks. Within their paper, Aslan, Aktuğ et al. make specific reference to a number of cyber risks which are most common, namely “Spyware”, “Scareware”, “Joke Programs”, “Ransomware”, “Hacking tools”, and “Remote access” (Aslan, Aktuğ et al., 2023). Such risks are a product of the ever-evolving nature of cyber attackers and the methods used by them. In tandem with this, it is also notable to mention the most common types of threats mentioned by Aslan et al. in their paper. These threats are; “Computer viruses”, “Computer worms”, “Trojan horses”, “Rootkits”, and “Hackers and Predators” (Aslan, Aktuğ et al., 2023). A study conducted by Alqahtani, Albalawi et al. (2023) revealed the most common cybersecurity threats and attacks to be Data Loss or Data Leakage, Denial of Service (DoS) or Distributed Denial of Service (DDoS) Attacks, Man-in-the-Middle Attack, Malware, Botnet Attack, Social Engineering, and Account Hijacking (Alqahtani, Albalawi et al. 2023). In this paper, the authors further noted that the CIA Triad (Confidentiality, Integrity, Availability) is most directly impacted by DoS and DDoS attacks. This is because in the case of such an attack, the organisation may lose access to any sensitive information stored on the cloud, rendering it

unable to operate effectively or at all, depending on the data stored and the nature of the organisation's business. Further to this, the research conducted by Alqahtani, Albalawi et al. (2023) identified 5 cybersecurity mitigation techniques that are suitable for cloud computing, these being; "Intrusion Prevention System (IPS) and Intrusion Detection System (IDS)", "Two-Factor Authentication", "Firewall", "Machine Learning", and "Data Encryption" (Alqahtani, Albalawi et al. 2023). Out of these five mitigation techniques, the IPS or IDS was the technique most mentioned in the studied research papers. Through this research, Alqahtani, Albalawi et al. (2023) concluded that the most common forms of cybersecurity threats were Data Breaches. For this reason, they have developed a platform named Automated Cloud Security Awareness Program (ACSAP) through which an organisation may minimise human error within an organisation's operations, this being identified as the prime cause for data breaches. In their conclusions, the authors remark on the significant lack of awareness of cloud computing security being addressed in literature. They outlined this as a gap, suggesting further studies are conducted on this topic to fix this issue.

In consideration of the risks and threats mentioned in the above papers, the essence of the above-mentioned cybersecurity risks and threats all lead to an organisation's loss of information to, or restriction of information by third party attackers. Many of the risks mentioned directly regard attackers limiting an organisation in its operations through the manipulation and/or disruption of its operational systems. This could also result in the permanent loss of the organisation's data, significantly affecting its operability. On the other hand, such attacks would also lead to stolen or leaked data to the attackers. This would infringe upon its customers' GDPR rights. Such cases would result in the organisation to suffer from harsh fines and penalties from its relevant authority and regulator/s.

From the above literature, it can be seen how although similar in nature, different academics have identified different cybersecurity risks. The identification of such risks answers exploratory question '**EQ4:** What are the most common cloud computing cyber security risks for organisations?'.

2.6. The role of cyber security in organisational resilience

When one considers the continuously digitalised world we live in, it can clearly be seen how cyber security has become an essential function for the successful survivability of any organisation. Organisations must ensure adequate governance of their cybersecurity policies, procedures, and measures so that they may effectively manage their cybersecurity risks (Mijwil, Filali et al. 2023). The previously mentioned cyber risks provide a good overview of the various organisational aspects that are affected by these risks, thus indicating the importance of cyber security in managing these risks to ensure business continuity. In following this train of thought, it should be noted how Hepfer, Powell et al. (2020) argue that cyber security should be treated as a means for an organisation to develop, not only for the mitigation of cyberattacks, but also as a means of identifying other organisational weaknesses and potential opportunities (Hepfer, Powell, 2020). As such, organisations should view cyber security as a tool for effective strategic development and implementation. In turn, this allows further organisational resilience. In their paper Garcia-Perez, Cegarra-Navarro et al. (2023) explore, through empirical research, the main elements necessary for healthcare systems to be able to adapt to and adopt the various new technologies entering the health industry. Within their study, they identify "cyber security knowledge development" (Garcia-Perez, Cegarra-Navarro et al., 2023) as one of the fundamental tools for ensuring "digital resilience" and sustainable transitions towards these new technologies. Bell, Partner et al. (2017) further enforce this train of thought through their definition of cyber resilience by explaining how "Cyber resilience is the ability to prepare for, respond to and recover from cybersecurity incidents." (Bell, Partner, 2017). However, cyber

security should not simply be considered as a stand-alone tool to be analysed at an independent level. On the contrary, it should be viewed as an integral and essential component, intertwined within the greater mechanism that is an organisation. This, paired with an increasing number of cyber security breaches (Rothrock, Kaplan et al. 2018), further emphasises the increased importance of organisations having adequate investment in cyber security.

By understanding the nature and importance of cyber security for organisational resilience, we have answered this study's fifth exploratory question; '**EQ5:** Why is cyber security important for the survivability of businesses?'

2.7. The construction of RQ2:

Through EQ4 and EQ5, it was shown how the world of cloud computing cyber security contains various risks which, if not adequately managed, could result in the bankruptcy of any organisation. Considering this, and following the concluding remarks made by Alqahtani, Albalawi et al. (2023), it is seen that more effective solutions are required to address the lack of cyber security awareness for cloud-based systems. To this extent, the second research question of this study was developed:

RQ2: To what extent do review articles address the awareness, or lack of awareness, of employees on cloud computing cyber security?

It can be a common error that when it comes to topics such as cloud computing and cyber security, that are of a digital nature, literature may tend to address these topics solely through the lens of the technical computing operations side and thus, may forego other less technical approaches such as governance and management solutions. Therefore, RQ2 will allow us to identify the extent to which academic literature addresses such non-technical approaches. This

would also allow this study to identify areas which are not addressed by literature, but which are still of significant relevance to the security of cloud computing.

2.8. The concurrent legislation and regulation at EU level that govern cyber security.

The interconnected world we live in today is heavily centralised around technology. This digital world is filled with various opportunities as well as multiple risks of a technological nature. In fact, European Regulators clearly state how such technologies “play a vital role in society and have become the backbone of economic growth.” (The European Parliament and the Council of the European Union, 2019). Due to these many digital factors, cyber security has become an essential part for any nation. The most effective way for competent authorities to manage the cyber security of their nations and the actors within them are through regulation and legislation. Such regulations are essential for numerous reasons. Firstly, regulation allows authorities to ensure the protection of citizens’ personal data. EU regulation such as the General Data Protection Regulation (GDPR) enable people to have control over their private data, as well as provides them with peace of mind that organisations handle such data in a responsible manner. This is essential for ensuring trust between individuals and organisations, whilst also promoting prudent use of data and digital tools. Cybersecurity regulation also allows for the safeguarding of national security. Cyberattacks also threaten the financial integrity of national economies, organisations, and individuals but through regulation, EU regulators aim to mitigate this as well. Finally, such regulations promote further research and innovation on cyber security between competitors, each one looking to further improve their security and benefit from a competitive advantage in doing so. This further enhances the security of EU countries as a whole and mitigates the risks associated with the digital world.

As explained above, regulations are an essential tool of EU regulators for preserving member states against cybersecurity threats and risks. The European Parliament makes reference to the concept of ‘digital transformation’, defining this as “the integration of digital technologies by companies and the impact of the technologies on society.” (European Parliament, 2021). The European Parliament makes reference to two specific EU regulations which specifically cater for this digital transformation through the protection from cyber threats (European Parliament, 2022). These two regulations are the Network and Information Security (NIS2) directive and the Digital Operational Resilience Act (DORA). The NIS2 directive, an expansion of the former NIS directive, is an EU-wide regulation intended to promote “a high common level of cybersecurity across the Union” (European Parliament 2023). The EU’s Network and Information Security (NIS2) Directive, and its predecessor the NIS Directive require users of essential digital services to implement robust security measures with the aim of protecting nationally significant infrastructure and information. On the other hand, the EU’s Digital Operational Resilience Act (DORA) is a forthcoming regulation specifically intended for ensuring the digital resilience of organisations, namely those operating within the financial services industry (Clausmeier 2023). The DORA demands that organisations have robust cybersecurity measures and incident response capabilities in place. Such requirements allow the EU to ensure organisations are capable of swift and effective recoveries from cyber incidents. DORA “entered into force on 16 January 2023” and “will apply from 17 January 2025” (Joint committee of the European Supervisory Authorities 2023). Considering the future application of this directive, it is still in the development phase, with the first and latest set of technical standards being made available for public consultation on 19 June 2023 (European Securities and Markets Authority 2023). A paper written by Clausmeier in 2023 provides an overview of its key rules and whether these are adequate in addressing the various cyber risks faced by financial services organisations (Clausmeier 2023). Clausmeier’s final remarks in this paper conclude that although there are still areas where the DORA needs improvement, “the risk-based approach of DORA will lead to a balanced application of the requirements.” (Clausmeier 2023).

Therefore, it is seen that EU regulators view the NIS2 directive and the DORA directive as the two core regulations for the protection against cyber threats, including cloud computing cyber security. This addresses the sixth exploratory question of this study: '**EQ6:** How are EU regulators currently addressing cloud computing cyber security within member states?'

Chapter 3. Methodology

This chapter provides an overview of the methodology used for conducting this research. Chapter 3.1 explains the reasoning behind the creation of the Exploratory questions outlined in Chapter 1. Chapter 3.2 explains the research strategy that was used, together with the inclusion and exclusion criteria considered. Chapter 3.3 provides an overview of the screening process for assessing the quality and eligibility of the literature for determining which studies were included within this study. Chapter 3.4 explains the methodology employed for extracting the data from the selected primary literature. In Chapter 3.5, the measures taken to assess the risk of bias within the chosen primary studies is explained. Chapter 3.6 explains the methodology undertaken in synthesising the data following the data extraction phase. Finally, Chapter 3.7 explains the measures taken for avoiding biases during the data collection and analysis phases.

3.1. Determining the exploratory questions

In creating the research questions for this research, a number of exploratory questions were first established and were used to guide the preliminary literature review.

EQs 1,2, and 3 were set with the aim of developing a general understanding of cloud computing, cyber security, and their interconnectedness. EQ 4 was designed with the aim of acquiring an understanding of the main cybersecurity issues faced by business organisations using cloud computing. EQ 5 was created as it is necessary to understand why cyber security is important of business organisations. This question helped in establishing the validity of this research. Finally, EQ 6 was established to obtain insight on the concurrent regulatory standpoint on cloud computing cyber security within the EU. This also provided insight into the future directions of EU regulation on this topic.

3.2. Research strategy and criteria

The objective of this study is to assess, through academic literature, the identified gaps and concurrent developments on cloud computing cyber security. By assessing the concurrent and future literature gaps and research directions, this study may serve as a guide for future studies on what areas require further research.

This study will target concurrent literature and its discussions on the topic of cloud computing cyber security. This means that the included literature would need to be assessed in a systematic manner to allow for unbiased and representative results. For this reason, a systematic literature review was determined to be the most effective way of achieving the set goals. This is because, when conducted in the proper manner, a systematic literature review provides the reader with a “transparent, complete, and accurate account of why the review was done,” how the review was done, as well as what was found through the study (Page, McKenzie et al. 2021). Systematic Literature Reviews are significant in that they allow the author to portray an unbiased and rigorous summary of concurrently available literature (Nightingale 2009). Implementing such a methodology for this research shall ensure more accuracy and reliability of the findings through the inclusion of all studies that fall within the inclusion criteria, and thus greatly minimising the risks of biases and the under representation or mis-representation of literature.

The preparation and implementation of a systematic literature review can be a daunting task and, if not done properly, may still lead to inaccurate and unreliable results. For this reason, a proven methodical approach must be taken to ensure this study is done properly. Although primarily designed for systematic reviews on topics within the medical sector, the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA), complemented by its 27-

item PRISMA Statement, is a methodological checklist-based guideline suitable for guiding systematic literature reviews of various natures (Page, Moher et al. 2021). Being a systematic literature review, this research thus follows the 27 items found within the PRISMA 2020 Checklist.

When consulting any one source for academic literature, one may be presented with numerous results of varied natures, and although each study is significant in its own right, not all would be significant for this specific research. For this reason, it is important to define a number of criteria for determining which literature is included for the purpose of this study, and which literature should be omitted.

This research aims to develop a better understanding of the concurrent literature gaps in discussing the cyber security of cloud-based systems. This means that the academic literature which is to be included within this study must discuss this topic. To ensure this, the following Table 3.1 shows the inclusion and exclusion criteria that were used to determine which studies were included in this research and which were not relevant to this study and were thus omitted from the data set to be assessed within this review.

Table 3.1: Table of Inclusion and Exclusion Criteria and their justification.

No.	Inclusion Criteria	Exclusion Criteria	Reasons
1	The study must be freely accessible as a full version of	Studies will be omitted if they	By only including papers that are open-access or

Table 3.1: Table of Inclusion and Exclusion Criteria and their justification.			
	the study either as an open access study, or through the resources provided by the University of Malta.	are inaccessible due to a paywall.	freely accessible as a University of Malta Student, this study would allow for the thorough examination of these papers, as well as ensure the replicability of this research and the findings therein.
2	The study must be written in the English language.	Any studies not written in the English language.	By regarding only studies written in English, it can be ensured that an accurate understanding of the studies can be achieved and that there would be no misinterpretation as a result of translations of papers.
3	Literature which discusses the relationship between cyber security and cloud computing	Any literature which does not discuss the inter-relation between	This ensures that included studies are relevant to this study.

Table 3.1: Table of Inclusion and Exclusion Criteria and their justification.			
		cyber security and cloud computing.	
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 discuss both topics, or that discuss only one topic in isolation, without regarding the other.	This is to ensure that the study discusses both cyber security and cloud computing within the research study.
5	Literature which was published in 2023, up to and including July 2023.	Literature which was published prior to 2023, or after July 2023.	With both cloud computing and cyber security being rapidly evolving topics, this ensures that the latest developments are taken into consideration for this study.
6	The study must be a literature review.	Any studies which are not literature reviews or which do not	The analysis of literature reviews allows for the assessment of the various conclusions

Table 3.1: Table of Inclusion and Exclusion Criteria and their justification.			
		explain the methodology adopted for their study.	brought about by these studies and in turn, by the various literature that each study encompasses. By checking that a sound methodology is explained, it allows for the assurance of good quality literature reviews.

Google Scholar and Scopus were the two databases used for identifying the studies to be used for this research. The rapidly evolving nature of cloud computing cyber security means that from one year to the next, academics would have progressed in addressing the multitude of research gaps on the topic. This study aims to address the concurrent literature gaps on the topic and for this reason, it was deemed ideal that the included literature must have been published in 2023, up to July of 2023. This would allow for the assessment of the latest developments on the topics. Furthermore, as mentioned in the inclusion criteria above, only literature review articles were regarded within this research. The reason behind this is that literature reviews would all have encompassed concurrent literature and boiled down the essence of these research papers into their results, discussions and conclusions. This would thus help in generating a representative sample of concurrent literature on the topic.

In consideration of the above-mentioned criteria, the following research strategy was implemented for this study:

The search terms used within the Google Scholar database were:

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

The results originating from this search consisted of various forms of research studies and methodologies. For this research, only review articles were included and so, the above search was further filtered to only show review articles which were published in 2023.

The search terms used within the Scopus database were:

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"))

The above search term for the Scopus database yielded 8 results in total. This low number was achieved as the database search allowed for the narrowing down of the search terms in a way that the resultant literature would have a greater chance of fitting within the inclusion criteria set above.

For both databases, all of the results generated were then reviewed and it was ensured that the final set of studies were compliant with the set inclusion criteria. This was done through the screening process explained in section 3.2.

3.3. Screening process

The quality and eligibility of the search results generated by the set terms were assessed through an initial review stage which was conducted manually, by a single person and through no automated software. For each result, the following process was followed for determining the final data-set to be included in this study:

Firstly, any duplicate studies were removed, and in the cases where a study was published in more than one source, the most recent version was considered. Following this, an eligibility assessment was conducted on the basis of the inclusion and exclusion criteria set in section 3.1. At this stage it was also ensured that each research paper was written in the English language and that the full text of each study is freely accessible either to the general public or through the resources provided by the University of Malta. Finally, each study was screened and it was ensured that the study was relevant to our research in that it discussed the inter-relation between cyber security and cloud computing.

3.4. Data extraction process

This section explains the methodology employed for extracting the data from the primary literature. First, each study was manually reviewed and notes were taken on the topics that were addressed and the conclusions that were made. These notes were recorded through a Table 4.1. Furthermore, a similar methodology was used where the papers were mapped according to the recommendations made for future studies. This mapping was recorded through Table 4.2. These two tables, shown in chapter 4.1. as Table 4.1 (a) and (b) and Table 4.2 (a) and (b), allowed for a more methodical comparison of the results presented in each study. These would be the two tables which were used for the data synthesis, detailed in section 3.5.

The main information which was recorded in each study were: the title and authors of each study, the focus of each study and its motivation, the future recommendations and directions identified by each study, and whether each study identified/provided one or more solutions to enhance cloud computing cyber security or if the study only identified gaps and issues. This data extraction process was completed manually by one person.

3.5. Assessing risk of bias in the included research studies

Assessing the risk of bias is an essential part in analysing literature as it allows for the assurance of a study's quality. At the Screening stage, each prospective study was reviewed briefly. Within this initial review, the risk of bias was mitigated through inclusion criterium number 5, ensuring that all included primary studies were literature reviews conducted through a sound methodology. A structured approach would inherently mitigate the risk of bias through its objectivity and so, inclusion criterium number 5 would provide better confidence that primary studies have a lower risk of bias. Furthermore, it was also ensured that each study was had more than one author. This reduced the risk of bias as multiple authors would have checked each other's work and would have identified and fixed any areas of potential bias.

3.6. Data synthesis methodology

The data synthesis followed a structured methodology. Firstly, each paper was thoroughly reviewed and critical information was noted for each study. Such information included, the topic addressed in each study, the main points made by each study, and the suggestions made for future works by each study. After this initial data extraction, two tables were constructed for the data synthesis of the primary studies. These two tables were used to Map the studies based on the topics discussed, and based on the future research identified by the two studies. These two tables allowed for the categorisation of literature based on the topics they addressed, as well as

based on the future recommendations brought forward by them. This methodology also made it possible for the collection of the data necessary for the answering of this study's research questions. RefWorks was used for storing and managing the references, as well as for managing the primary literature of this study.

3.7. Measures for avoiding bias in the data collection and analysis phases

As a measure for avoiding bias, the PRISMA checklist was followed systematically. This methodical approach allowed for the assurance of objectivity within the data collection and analysis phases. Furthermore, a systematic approach was employed through the use of Table 4.1 and Table 4.2. For each study, all of the required information explained within section 3.3. was recorded into the table. This ensured that for each study, the same forms of data were recorded. The majority of the information required was methodically gathered through a detailed review of each study's results, discussion, future recommendations, and conclusions sections.

Here, it was also ensured that data recorded within the table was written in the same fashion as in each relevant study. This ensured that no data in written incorrectly due to a different interpretation that that given by its own authors. Furthermore, a conscious effort was made to ensure that each study was reviewed through an objective view, assessing purely what the authors discussed, and no subjective ideologies influenced the data extraction and interpretation.

Chapter 4. Results

This chapter provides an outline of the results achieved from the analysis of the primary literature identified. Chapter 4.1 explains the procedure that was followed in identifying the study's primary literature. Chapter 4.2 outlines the main points brought about by each primary study and identifies any commonalities between the topics of the papers. Chapter 4.3 further outlines the key gaps and future directions identified by each paper.

4.1. Selection of Primary Literature

The selection process for acquiring this study's primary literature followed the format of the PRISMA 2020 Flow Diagram. First, the search terms were used to identify the first set of results from Google Scholar and Scopus. This resulted in a total of 61 studies. These results were then screened and only those studies that fit within the inclusion criteria, and were relevant to this study were kept as primary studies. This was ensured through a thorough screening process where each paper was reviewed, keeping in mind the scope of this study. This resulted in a total of 11 Primary Literature studies which were chosen for further analysis through this study. A Flow Diagram depicting this process was developed and followed for this study. This flow diagram is presented in the below Figure 4.1.

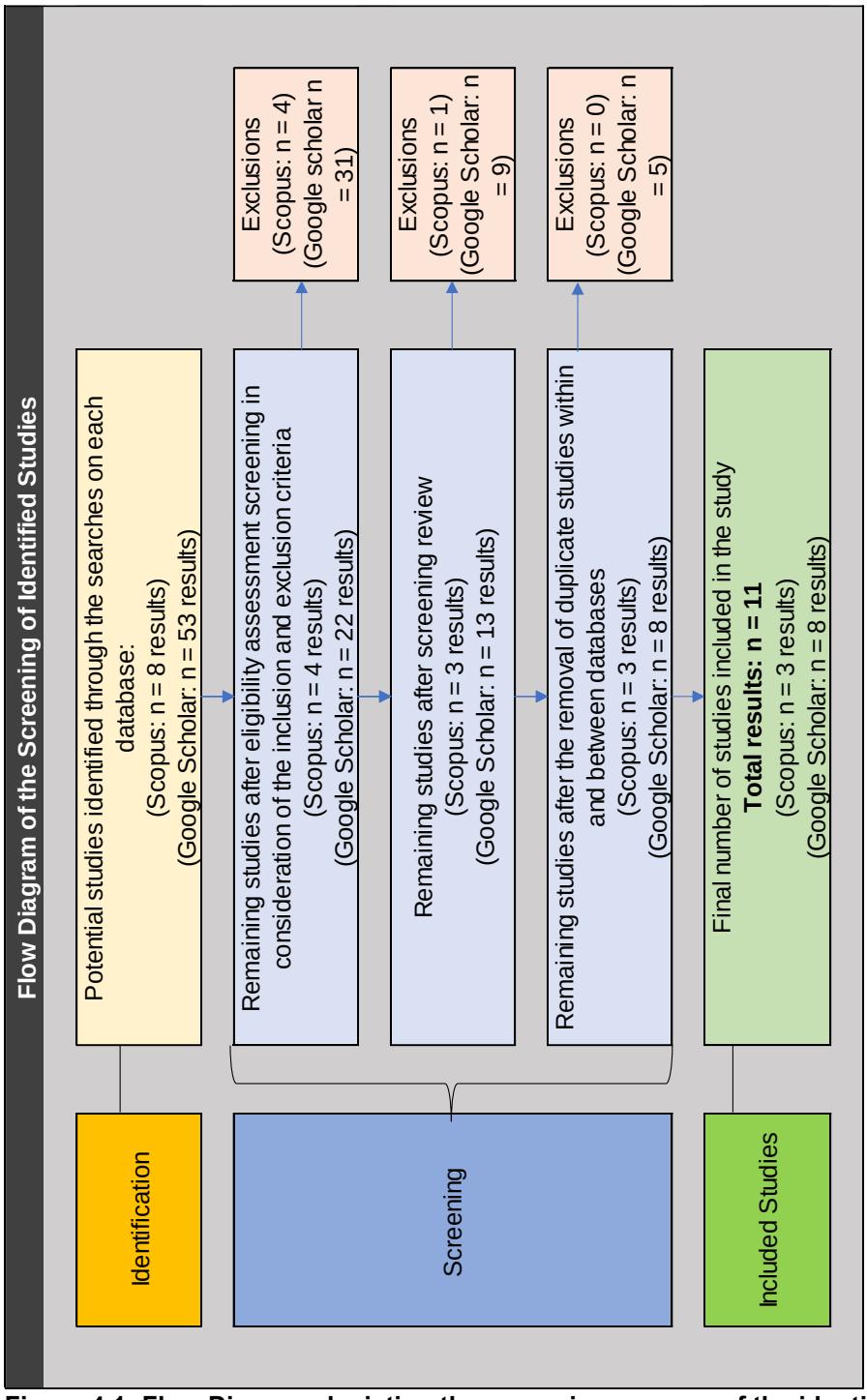

Figure 4.1: Flow Diagram depicting the screening process of the identified studies

As it is shown in the above Figure 4.1, the initial search for the Google Scholar database yielded a total of 53 papers, whereas the initial search for the Scopus database yielded a total of 8 papers. After the screening process, we were left with a total of 8 papers from Google Scholar and 3 papers from Scopus which fit into the inclusion criteria.

4.2. Analysis of results

Following this selection process, each primary study was reviewed thoroughly and a series of critical data points were identified for further review and the answering of this paper's research questions. The studies were thoroughly reviewed and two tables were constructed, classifying each paper based on the topics addressed by it. This table is shown below through Tables 4.1.(a) and 4.1.(b).

Table 4.1.: Table of topics discussed by each identified study (showing the first 6 studies)

Mapping of identified studies by Topic Discussed							
Paper		(Soveizi, Turkmen et al. 2023)	(Can, Thabit et al. 2023)	(Naseri, Kazemi et al. 2023)	(Komar, Patil 2023)	(Kwao Dawson, Twum et al. 2023)	(Jha, Kumari et al. 2023)
Topic Discussed by the study	The need for more robust and better understanding of cryptographic algoritms for the encryption of cloud data.		X			X	
	Lack of focus on the security of cloud-based Workflow Management Systems	X					
	The lack of literature discussing Cloud Battery Management Systems (CBMS).			X			
	Challenges faced by organisations in their adoption and use of cloud computing				X		X
	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)						

Table 4.2.: Table of topics discussed by each identified study (showing the remaining 5 studies)

Mapping of identified studies by Topic Discussed						
Paper		(Rahaman, Islam et al. 2023)	(Pawlicki, Pawlicka et al. 2023)	(Minna, Massacci 2023)	(Kwao Dawson, Twum et al. 2023)	(Surianarayanan, Chelliah 2023)
Topic Discussed by the study	robust and better understanding of cryptographic algoritms for the encryption of cloud				X	
	the security of cloud-based Workflow Management					
	literature discussing Cloud Battery Management					
	by organisations in their adoption and use of cloud computing					
	solutions and tools for improving the security of microservice architectures and cloud-native	X		X		
	cloud computing systems with emerging technologies (such		X			X

Through the analysis of the chosen primary literature, six topics were identified between the eleven papers included. The above Table 4.1 provides an indication of the most commonly addressed topics by literature reviews. The following section shall provide a brief overview of the papers' discussions in light of these six topics.

4.2.1. Cryptographic algorithms for the encryption of cloud data

Data security is a commonly discussed topic when it comes to cloud computing cyber security. The core items presented by the CIA triad (Confidentiality, Integrity, and Availability) are essential factors for ensuring this data security. In light of this, Jha, Kumari et al. (2023) notes that various academics are opting to utilise encryption cryptography as the main means of ensuring data security (Jha, Kumari et al. 2023). This research strengthens this claim by identifying three literature review articles that directly address algorithm cryptography as a means of developing data security within the cloud.

Can, Thabit et al. (2023) considers encryption to be “the primary component of data security” (Can, Thabit et al. 2023). In their paper, they employ a 5-step Literature Review methodology to address information security challenges by studying and analysing the innovative technology of genetics based cryptographic algorithms. They discuss the various forms of cryptography and sub-divides cryptography into three classifications: Traditional Cryptography, Lightweight Cryptography, and Genetics Cryptography (Can, Thabit et al. 2023). Here, they explain each category, and go into considerable detail on a form genetic cryptography called DNA cryptography. They explain how this innovative technique combines classical cryptography techniques with biological DNA concepts to achieve a more efficient, faster, and less resource consuming encryption technique. Furthermore, they outline how genetic cryptography addresses the shortcomings of present cryptography algorithms. In essence, they outline how DNA cryptography provides algorithms that, by mimicking the biological processes present in DNA, are more complex and thus, more secure. Their study concludes that although it “is still in a nascent state” (Can, Thabit et al. 2023), genetics cryptography provides a more robust solution to the increasing need of data security within cloud computing. As such, they suggest

that further studies should be focused on the further development of DNA cryptography, specifically in the IoT environment.

Kwao Dawson, Twum et al. (2023) also address the use of cryptographic algorithms in two papers identified within this study. Their papers, one published on the 31st March of 2023 and titled; “RECONNOITERING SECURITY ALGORITHMS PERFORMANCE IN THE CLOUD: SYSTEMATIC LITERATURE REVIEW BASED ON THE PRISMA ARCHETYPE”, and their subsequent paper published on the third of July of 2023 and titled; “PRISMA Archetype-Based Systematic Literature Review of Security Algorithms in the Cloud”, aimed to understand the various cryptographic tools and methods discussed in literature. Through these systematic literature reviews, the authors also intended to assess the impact of these various cryptographic tools on cloud computing of cyber security. These studies also allowed them to outline the main concerns on cloud computing cyber security as well as allowed for the identification of numerous security techniques used to secure cloud data, namely firewalls, data masking, encryption, and Blockchain. Of these, their studies identified the use of encryption algorithms as being “the best approach to ensure cloud security” (Kwao Dawson, Twum et al. 2023). Furthermore, the research managed to identify a number of security challenges present within cloud computing. In both papers, the authors outlined how these challenges primarily revolved around the CIA Triad, i.e. data confidentiality, data integrity, and data availability, being compromised. For each of these challenges, they identified approaches for rectifying them within their first paper. Finally, the authors noted in both papers that although an organisation’s shift to cloud computing can bring with it various benefits to both the organisation and its customers, security concerns are hindering the full adoption of cloud computing.

Through these conclusions, their first study noted that further efforts should be directed towards understanding and addressing the various issues hindering the growth and adoption of cloud computing. They noted that future research should focus on “data security, data privacy and confidentiality, reliability and trust, and multi-tenancy on the cloud by employing algorithms that have nonlinear time complexity, unpredictable execution time, and low execution as they happen to the least researched” (Kwao Dawson, Twum et al. 2023). Their subsequent study published in July 2023 outlined the inadequacy of concurrent cryptographic techniques in addressing the various contemporary security threats faced by cloud computing users due to the limitations and predictability of their linear run times. In light of this, the authors outlined two core suggestions for addressing these issues. Firstly, the note how cloud computing service providers should use non-linear algorithms as opposed to linear algorithms for their security schemes. Furthermore, they suggest that device manufacturers should also make use of non-linear algorithms. The implementation of these suggestions by the relevant stakeholders would greatly address the limitations currently posed by linear cryptographic techniques. Through their study, Kwao Dawson, Twum et al. (2023) further suggest should be addressed by future academic studies. Firstly, it was noted that further research should be focused on non-linear algorithms. Secondly and in complement to their prior paper, the authors note that further studies should be directed to address the various challenges posed by cloud computing namely, issues on data confidentiality, multitenancy, and data reliability.

4.2.2. Cloud-based Workflow Management Systems

In today’s world, businesses operations have become increasingly dependent on data and computing intensive processes and the world of cloud computing is no exception to these developments. The paper of Soveizi, Turkmen et al. (2023), state that security, or rather security concerns, are a significant inhibitor of businesses’ adoption of cloud computing. This is especially so in the cases of business workflows that deal with sensitive information. Through

their paper, Soveizi, Turkmen et al. (2023) address this issue. Their study was made to develop an understanding of how such security concerns in scientific and business workflows in cloud environments are being addressed in literature. Through this literature study, the authors further aim to outline the key literature gaps on this topic (Soveizi, Turkmen et al. 2023). The core motivation for their study was that the authors identified a gap in literature as there were no studies identified which address the security and privacy concerns in cloud-based business or scientific workflows.

Through their study, a number of literature gaps were outlined. Firstly, the authors identified that for both business and scientific workflows, there exists a lack of literature that addresses the monitoring, analysis, and adaptation phases of these workflows. As such, it was outlined how existing literature tends to focus more on the modelling stage of these workflows, and less on their execution stage. Additionally, the authors also identified a lack of literature which addresses the need for “reliable and scalable approaches that can detect, prevent and react to security violations and compensate for part or all of the damage” in the case of both scientific and business cloud-based workflows (Soveizi, Turkmen et al. 2023). Through their findings, they conclude that in the case of both scientific and business workflows, there are no workflow management systems that cater for cloud-based infrastructures and that cater for the security needs of the entire workflow life cycle.

These conclusions identify significant gaps in literature pertaining to workflow management system security and so, the authors suggest that future research should be dedicated to enhancing existing literature with the aim of developing methods and workflow management systems that are capable of addressing the security concerns of cloud-based workflows during their entire lifespan.

4.2.3. Cloud Battery Management Systems (CBMS)

The application of cloud computing infrastructure extends further than just a means of improving organisational operations. Naseri, Kazemi et al. (2023) remarks on the advancements of cloud computing leading to the development of Cloud Battery Management Systems (CBMS). They define CBMSs as “a cyber-physical system with connectivity between the physical BMS (Battery Management System) and a cloud-based virtual BMS, which is realized through a communication channel such as Internet of Things. The integration of Battery Management Systems with the cloud creates great potential for more efficient and superior performance however, the cloud-inherent cyber security challenges, paired with the uses of BMSs, namely for Electric Vehicles (EVs), means that faults in CMBSs could result in critical failures that are potentially life-threatening. Therefore, Naseri, Kazemi et al. (2023) conducted their study to review and assess the cyber security of BMSs and CBMSs. Such a study would enable further understanding on the concurrent literature discussing CBMSs, which is a relatively innovative technology. Their study initially reviewed the potential attack types and scenarios relevant to CBMSs and outlined three main classifications of attacks namely; confidentiality, integrity, and availability attacks. They further analysed potential attack paths and in doing so, they identified numerous vulnerabilities both from “in-vehicle communications”, as well as “extra-vehicle communications” (Naseri, Kazemi et al. 2023). Such vulnerabilities would have significant impacts of varying natures. Malicious cyber-attacks could result in functional damages to the CBMSs and the EVs. Such attacks could also result in financial damages as cyber-attacks could contribute to a faster battery degradation than intended. Furthermore, confidentiality attacks could compromise the privacy of users for example through the GPS system, as well as lead to the stealing of confidential data on the specifications of the BMS. Another critical impact that could result from cyber-attacks is the compromise of CBMS safety measures, thus exposing EV users to great risk of accident. Finally, the authors also identify how such vulnerabilities can result in the corruption of data through cyber-attacks which would compromise the integrity of CBMS databases (Naseri, Kazemi et al. 2023). Considering such

impacts, the authors attempted to address these vulnerabilities by outlining a number of methods for managing these attacks through detection and mitigation, as well as by identifying areas of improvements which would result in better CBMS cyber security. Furthermore, it was noted that, although “standards such as SAE J3061 and ISO 21434 provide useful guidelines to address this topic,” (Naseri, Kazemi et al. 2023) there exists a lack of standardisation on CBMS cyber security infrastructures.

Through this study, the authors concluded that BMSs are critical for ensuring the functional safety of EVs, and that CBMSs should be used for complementing the performance of these BMSs. They also note “the great potential for the marketability of this technology” (Naseri, Kazemi et al. 2023) yet, a number of gaps still exist which warrant the need for further research in the future. Firstly, the authors identify the need for establishing a better understanding of the various cyber threats and their effects on CBMSs and EVs. They suggest that this is achieved through the conducting of a Threat Analysis and Risk Assessment (TARA). The authors also highlight the emerging nature of the CBMS technology by outlining the need for further research to be conducted on the means of analysing, testing, and validating BMS and CBMS cyber security designs, the development of algorithms that are capable of addressing the cyber security needs and challenges of CBMSs, and for CBMS cyber security to be explored further in different lifecycle stages of the CBMS. The authors also suggest that further research is dedicated to the improvement of the implementation of CBMS systems, as well as the use of AI for enhancing security in these designs. It was also recommended that further systematic reviews are conducted to help develop a better understanding of various CBMS cyber security topics. Furthermore, standardised regulations should be established for improving the overall cyber security of the CBMS industry as a whole. (Naseri, Kazemi et al. 2023)

4.2.4. Challenges faced by organisations in their adoption and use of cloud computing

Cloud computing is a new and innovative technology which presents revolutionary solutions to existing organisational challenges. Thus, it can be understood that various organisations are starting to look towards integrating cloud computing services within their operations. However, while cloud computing does offer various advantages, there exist numerous obstacles and challenges that hinder organisations from adopting this technology.

Komar and Patil (2023) outline three key challenges faced by organisations in their adoption of cloud computing. Organisations must manage data security and privacy as this is one of the challenges in cloud-adoption. Here, organisations must make use of access control and authentication controls to mitigate such security threats (Komar, Patil 2023). Furthermore, organisations must also ensure that they are in compliance with the various data protection and privacy laws applicable to them, such as the General Data Protection Regulation (GDPR) (Komar, Patil 2023). Failure to manage such compliance risks could result in various repercussions such as fines, lawsuits, and, depending on the gravity of the situation, imprisonment of the negligent parties, amongst other consequences. The limitations posed by vendor lock-in are the third challenge outlined by the authors. Vendor lock-in refers to the case “where organizations become highly dependent on a specific cloud provider's service” (Komar, Patil 2023), thus limiting the organisations’ flexibility for data portability through the migration of data either to different service providers, or back to an on-site computing infrastructure (Komar, Patil 2023).

A significant challenge which also hinders cloud adoption is the lack of awareness by individuals and organisations on the various risks and the importance of IT security inherent to the cloud (Jha, Kumari et al. 2023). The study conducted by Jha, Kumari et al. (2023) aimed to address

this issue by outlining the main procedures known for ensuring data security within the cloud, as well as the methodologies employed for authorising these procedures. Their results identified the use of encryption methodologies as the most discussed control for ensuring data security within cloud environments, followed by the establishment of guidelines and of frameworks as being the second and third-most common controls respectively. From these papers, the authors also noted that a vast majority (42%) of the papers which had proposed a methodology for ensuring data security did not back up their claim through any form of validation process, with a further 32% making use of experimentation for validating their proposed methodology. This lack of validation could indicate the need for more future research to incorporate validation techniques to support their proposed methodologies and theories.

These various hinderances on the mass adoption of cloud computing services outline a number of key recommendations which should be addressed by future research. Firstly, it is recommended that further research should address the integration of emerging technologies such as AI, IoT, Cloud Computing, and Edge Computing, for an overall better cyber security of these technologies (Komar, Patil 2023). Further research should also be dedicated to develop a better understanding of the various security issues prevalent in cloud computing infrastructures, as well as on the development of frameworks and standards to be followed for enhancing the cyber security of this technology (Komar, Patil 2023). Komar and Patil (2023) also note the need for future research to address the sustainability aspect of cloud computing through the development of more sustainable cloud-based infrastructures. Additionally, further research should also be dedicated to the optimisation of serverless computing architectures. Finally, further developments should be made on improving cyber risk management tools such that they would be able to keep up with the evolution of cyber risks (Komar, Patil 2023). Encryption was found to be the most widely used data security tool for the cloud (Jha, Kumari et al. 2023) and

so, future research should also be dedicated on improving this technology to keep it relevant in the face of evolving cyber threats.

4.2.5. Existing defensive solutions and tools for improving the security of microservice architectures and cloud-native systems

The expansive nature of cloud computing and microservice architectures have led to significant security challenges which organisations must overcome in order to effectively make use of such technologies. For this reason, research on defensive solutions and tools which would be used to manage such security challenges are crucial for the further adoption and growth of the microservices industry.

Rahaman, Islam et al. (2023) recognised this need and conducted a literature review through which they outlined the currently available and used defence mechanisms involving static analysis that can detect and react against attacks and vulnerabilities of cloud-native systems. Their study categorised the identified literature into five core topics that are discussed by academics in addressing the defence of cloud-native systems and these were; challenges related to microservice containers, challenges related to edge and fog computing, systematic literature reviews on the topic, challenges for practitioners of cloud-native systems, and challenges in the systems' design (Rahaman, Islam et al. 2023). Such classifications provide an indication of the most commonly discussed literature gaps which require further attention.

Through their comprehensive review, they concluded that concurrently used defence approaches revolve around the vulnerabilities and the security solutions of microservice containers. Furthermore, the note how "security design flaws, and detection mechanisms convincingly addressed several attacks: DDoS, CSRF, SQL Injection, XSS, and Replay" (Rahaman, Islam et al. 2023). The authors concluded that for addressing the increasing and

evolving security challenges present in cloud-native infrastructures, they aim to “develop a static analyzer that will implement a security defense solution addressing potential adversarial categorized attacks, detecting them, and mitigating” (Rahaman, Islam et al. 2023).

The study conducted by Minna and Massacci (2023) also contributed to the topic of existing defensive solutions and tools for improving the security of microservice architectures and cloud-native systems. Their study focused on finding and classifying available tools and techniques for evaluating, mitigating, and recovering from run-time security issues affecting microservices. This allowed the authors to address the topic of run-time security which was found to be poorly addressed by concurrent literature (Minna, Massacci 2023). Their study resulted in a number of conclusions. Firstly, it was outlined how the most notable gaps in literature lie on the topics of the orchestration architectural layer, the verification of security policies, as well as on the resilience of microservice architectures against threats and their recovery from attacks. The authors note how a large number of security solutions do not test the deployed systems’ security as expected. They further noted how there is a gap in literature when it comes to the reproducibility of security experimentation with testbeds, as well as security studies ‘in the wild’ and so, they recommend that future studies should address these gaps (Minna, Massacci 2023).

4.2.6. The integration of cloud computing systems with emerging technologies

Present-day technologies have come a long way from their initial stages, and have now become integrated within the technology industry. Through various advancements over time, emerging technologies have become inter-connected and inter-dependent. Given the integrated nature of various technologies today, it is no surprise to see that some of these technologies may have

certain commonalities. Threats are also a topic of commonalities between various emerging technologies.

Pawlicki, Pawlicka et al. (2023) identifies a lack of literature that addresses the threats common to Cloud computing, IoT, and Edge computing and so, they conducted a study with the aim of developing a catalogue of the identified attacks common to these three technologies, as well as a number of solutions and counter measures which would contribute to improving the security of cloud computing, edge computing, and IoT systems. Furthermore, their study assessed various papers and identified a number of security solutions for mitigating the security threats common to cloud, edge and IoT systems. The results showed that the attacks common to all three technologies were DoS and DDoS attacks, Eavesdropping, Man-in-the-Middle (MitM) attacks, and various forms of Malware such as viruses, trojans, and scareware attacks. In their assessment if these attacks and their included literature, the authors further outline a number of measures that were deemed to be ideal for managing these common attacks. The implementation of an Intrusion Detection System (IDS) was suggested for the mitigation of a large variety of attacks. Here, the authors further add that the integration of IDSs with Artificial Intelligence and Machine Learning (AI/ML) systems would further enhance the IDS. The use of encryption techniques was also recommended to ensure data confidentiality. The implementation of monitoring and scanning mechanisms were also suggested. Furthermore, their study identified a number of papers that suggested the use of ““traditional” firewalls and antivirus software” (Pawlicki, Pawlicka et al. 2023). In such infrastructure, human errors cannot be overlooked, and Pawlicki, Pawlicka et al. (2023) noted how academics recommend that organisations screen their employees and service providers to ensure their legitimacy and mitigate the chances of internal threats. Similarly, service providers should also have measures in place to prevent abuses from product users. Further recommendations identified from their study include the implementation and management of backup and recovery mechanisms,

ensuring organisational stakeholders maintain security and privacy, as well as the implementation of access control mechanisms.

In review of their study, the authors note how there is a lack of coherence in the terminologies used by academics in their studies. In light of this, the authors outline the need for future works to develop a unified and exhaustive catalogue containing the various forms of attacks which cloud computing, edge computing, and IoT systems are exposed to (Pawlicki, Pawlicka et al. 2023).

The integration of different technologies may also be the cause of new vulnerabilities within the integrated systems. Surianarayanan and Chelliah (2023) addresses these newly introduced vulnerabilities, specifically in the case of the integration of cloud computing and IoT infrastructures. Their paper highlights the security issues, and their suggested solutions, associated with cloud and IoT systems, as separate infrastructures as well as in their integration. Following this, they outline popular IoT-cloud platforms and how they facilitate secure integration. Finally, their study highlights a model for IoT and Cloud security based on a cooperative shared responsibility of IoT and Cloud service providers which allows for the assurance of security within cloud-based IoT applications. Through their study, the authors identify the role of “commercially available IoT-cloud platforms” (Surianarayanan, Chelliah 2023) that enable industries to overcome the onerous process of having to develop its own integration process, thus simplifying this integration. The authors further note how such commercially available IoT-cloud platforms also provide much needed solutions to the numerous security issues inherent to these infrastructures and their integration processes. Machine learning algorithms have become a useful tool for predicting and mitigating security threats, and cloud computing inherently allows for “centralized security monitoring and management”

(Surianarayanan, Chelliah 2023) and yet, IoT systems may still be prone to security threats such as “manual errors, insider threats, intruders, physical threats, and threats associated with third-party vendors and service providers themselves” (Surianarayanan, Chelliah 2023). Furthermore, Surianarayanan and Chelliah (2023) note how IoT’s projected development will require strong and comprehensive security measures which allow for the mitigation of emerging threats resulting from such growth. In light of this, it is recommended that future research is dedicated on developing such robust security systems, capable of addressing next-generation security threats (Surianarayanan, Chelliah 2023).

4.3. Outlined future directions

From Chapter 4.2, a number of research gaps for future considerations were outlined by the chosen primary literature papers. These gaps are summarised through the below tables 4.2.(a) and 4.2.(b)

Table 4.3.: Table of identified future recommendations for each identified study (showing the first 5 studies)

Mapping of identified studies by the future directions identified							
Paper		(Soveizi, Turkmen et al. 2023)	(Can, Thabit et al. 2023)	(Naseri, Kazemi et al. 2023)	(Komar, Patil 2023)	(Kwao Dawson, Twum et al. 2023)	(Jha, Kumari et al. 2023)
Future directions identified	Cryptographic algorithms and their application to emerging technologies.		X	X		X	X
	Further research on CBMS cyber security			X			
	Better regulatory standards and frameworks for better cyber security within the cloud	X		X	X		
	The integration of emerging technologies for better cyber security			X	X		
	Understanding the various security issues in cloud computing				X	X	
	Sustainability in cloud-based infrastructures				X		
	Optimizing serverless computing architectures				X		
	Better cyber risk management tools to keep up with the evolution of cyber risks.				X		

Table 4.4.: Table of identified future recommendations for each identified study (showing the remaining 5 studies)

Mapping of identified studies by the future directions identified						
Paper		(Rahaman, Islam et al. 2023)	(Pawlicki, Pawlicka et al. 2023)	(Minna, Massacci 2023)	(Kwao Dawson, Twum et al. 2023)	(Surianarayanan, Chelliah 2023)
Future directions identified	Cryptographic algorithms and their application to emerging technologies.				X	
	Further research on CBMS cyber security					
	Better regulatory standards and frameworks for better cyber security within the cloud					
	The integration of emerging technologies for better cyber security					X
	Understanding the various security issues in cloud computing		X	X	X	
	Sustainability in cloud-based infrastructures					
	Optimizing serverless computing architectures					
	Better cyber risk management tools to keep up with the evolution of cyber risks.	X				

From the above table 4.2, eight core literature gaps were identified from the included studies. The future requirements based on the identified gaps are; (1) the need for further research to be conducted on cryptographic algorithms and their applications on emerging technologies, (2) the need for a greater understanding on Cloud Battery Management Systems and their cyber security, (3) the need to have better established regulatory standards as well as the development of frameworks to be followed for enhancing cloud computing cyber security, (4) the need for further research to be conducted on the integration of emerging technologies for enhanced cyber security, (5) the need for further research to be conducted for understanding better the various security issues within cloud computing, (6) the need for further research to be dedicated on making cloud computing infrastructures more sustainable, (7) the need to further explore and optimise serverless computing, (8) and the need for developing better cyber security management tools capable of maintaining relevance in light of the rapid evolution of cyber risks.

Chapter 5. Discussion

This chapter shall provide an analysis of the results outlined in Chapter 4 in a general context of the overall results outlined, as well as in the context of addressing this study's research questions. Therefore, this chapter is organised as follows: Chapter 5.1 provides an overall analysis of the findings in the general context of all the findings. Chapter 5.2 addresses RQ1 of this study. Chapter 5.3 addresses RQ2 of this study. Through chapters 5.2 and 5.2, this study would achieve its objective of identifying future directions of cloud computing cyber security, as well as the future research directions related to this topic.

5.1. Analysis of the findings

Through the results obtained from this research, it was seen that the topic of cloud computing cyber security is expansive and that different academics are looking at this topic from different angles, each providing a unique view on the world of cloud computing cyber security. Furthermore, the results obtained identified numerous literature gaps that warrant the need for future research. From the analysed papers, it is notable to see how the theme of cyber risks and threats present within the world of cloud computing, commonly revolved around the enfeeblement of the CIA triad i.e., Data Confidentiality, Data Integrity, and Data Availability, thus leading to weaker cyber security infrastructures.

In analysing the included literature, it was also noted how the topics discussed were very coherent in their views of cloud computing and its cyber security, namely on how further research is required for academics and industry professionals to further enhance their understanding of this technology. The need and lack of such research, creates a level of uncertainty amongst industry practitioners that hinders the adoption of cloud computing. Both papers written by Kwao Dawson, Twum et al. (2023), as well as the papers of Komar and Patil (2023) and Jha and Kumari et al. (2023), all outline how the uncertainties on security mystifying

cloud computing is a core hinderance of a faster and wider adoption of this technology (Komar, Patil 2023, Kwao Dawson, Twum et al. 2023b, Jha, Kumari et al. 2023, Kwao Dawson, Twum et al. 2023a)

5.2. Identifying concurrent research gaps in cloud computing cyber security that should be addressed by future research

As previously outlined, uncertainty on the security of cloud computing is a main barrier to many organisations' adoption of cloud computing. This study's first research question seeks to address this issue by outlining the main research gaps identified by literature on cloud computing cyber security. The answering of this question would allow us to identify what literature gaps future research should address, thus aiding in the demystification of cloud computing and its security.

This study outlines eight core literature gaps on cloud computing cyber security which warrant the need for further research. An analysis of these research gaps outlines how certain gaps were mentioned in more papers than others. Through the below sub-sections, this RQ1 was answered by identifying the concurrent research gaps in cloud computing cyber security that should be addressed by future research.

5.2.1. Further research on various security issues in cloud computing.

One of the most commonly mentioned gaps which should be addressed by future research is the need for establishing a deeper understanding of the various security issues present in the world of cloud computing. Outlined by five out of the eleven papers included within this study, cloud computing security risks is a core hinderance in the adoption of cloud computing and

future research must address the uncertainties created by such gaps, to allow for a safer transition to cloud services by organisations.

5.2.2. Further development of cryptographic algorithms (such as Genetic and DNA cryptography) and their application to emerging technologies.

Five out of eleven studies also discussed the need for further research to be made on cryptographic algorithms and their applications to enhance cloud computing. The use of cryptographic algorithms has become a topic of interest for researchers through its ability to be used for encrypting sensitive data. Papers such as those of Kwao Dawson, Twum et al (2023), Can, Thabit et al. (2023), Naseri, Kazemi et al. (2023), and Jha, Kumari et al. (2023) all recognise the need for enhancements to be made on cryptographic algorithms, such as through the development of genetic and DNA cryptography (Can, Thabit et al. 2023), which will allow for more securitisation of cloud-based data.

5.2.3. The need for the establishment of better regulatory standards and further developments of frameworks to be followed for better cyber security within the cloud.

Another gap outlined for future studies is the need for more rigorous regulatory standards and frameworks to be established which are specifically designed to cater for the security needs of cloud-based infrastructures. Cloud computing is a relatively new technology, as well as a fast growing one, meaning that although organisations have not yet had the time to fully understand and become accustomed to this technology, rapid changes are constantly occurring within the technology, leaving numerous gaps. Through the establishment of cloud-specific regulatory standards (Naseri, Kazemi et al. 2023), as well as operational frameworks to be used within cloud-based infrastructures (Soveizi, Turkmen et al. 2023, Komar, Patil 2023), a more organised and secure approach to the adoption of cloud computing can be taken, potentially on a global

scale. An area which future research should explore is the extent to which the upcoming DORA regulation will help in addressing this issue.

5.2.4. Further research on the integration of emerging technologies (such as AI, IoT, Cloud Computing, and Edge Computing) for better cyber security.

The concurrent rate of technological developments is pointing towards the integration of various emerging technologies in organisational operations. This study has identified that this theme is also applicable to the world of cloud computing. Three papers were outlined in this study, that indicate the integration of cloud computing with emerging technologies like AI (Naseri, Kazemi et al. 2023, Komar, Patil 2023), IoT (Komar, Patil 2023, Surianarayanan, Chelliah 2023), as well as Blockchain, Quantum computing and Edge computing (Komar, Patil 2023). Much like in the introduction of cloud computing as an emerging technology, this integration is bringing forward both solutions to existing security issues, as well as the need for new security solutions to address emerging security gaps caused by such amalgamations.

5.2.5. Further developments on cyber risk management tools to keep up with the evolution of cyber risks.

Two papers identified within this study also outline the need for further research to be conducted on developing cyber risk management tools which are capable of staying relevant in light of the rapidly evolving cyber risks. It was outlined how intrusion detection and threat intelligence systems should be further developed to better cater for cloud computing infrastructures as well as for the constantly changing cyber threats (Komar, Patil 2023). Rahaman, Islam et al. (2023) also identified the need for cloud-tailored cyber risk management tools to developed. In light of this, they aim to address this issue by developing “a static analyser” “which would implement a

security defense solution that addresses potential adversarial categorized attacks, detecting them, and mitigating them" (Rahaman, Islam et al. 2023).

5.2.6. Other gaps recommended to be addressed by future research.

Although not as represented as other gaps, other gaps were identified by this review. The need for further research on CBMS cyber security is one such gap (Naseri, Kazemi et al. 2023). Although a niche topic, exclusively applying to Battery Management System (BMS) and Electric Vehicle (EV) cyber security, the need for ensuring adequate CBMS cyber security has global applicability. The importance of addressing this gap is especially highlighted in consideration of the growing electric vehicle industry world-wide. In their paper, Komar and Patil (2023) outline the need for further research to be made on improving cloud computing infrastructures. Given the extensive applicability of cloud computing, optimising its infrastructure is an essential undertaking for improving its operational efficiency. One area which was highlighted for future research was the optimisation of serverless computing architectures (Komar, Patil 2023). Such optimisation would allow for more efficient resource allocation, better performance, as well as enhanced scalability for Function as a Service (FaaS) platforms (Komar, Patil 2023). Furthermore, the research paper written by Komar and Patil (2023) outlines the need for future research to develop more sustainable and efficient cloud computing infrastructures. It was noted how such a gap was not outlined by any of the other included literature and yet, it is an important topic for future research to address given the increasing environmental awareness of governments, organisations, and individuals alike.

5.3. To what extent do review articles address the awareness, or lack of awareness, of employees on cloud computing cyber security?

Employees' lack of awareness on cloud computing cyber security is a significant problem which is found to be a core cause of poor organisational cyber security, leading to higher human error incidents and data breaches (Alqahtani, Albalawi et al. 2023). In addressing RQ2, this study has analysed the core topics addressed by the included reviews, and assessed the extent to which each topic addresses this gap outlined by Alqahtani, Albalawi et al. (2023).

Jha, Kumari et al. (2023) recognises this lack of awareness as a risk and attempt to address it through their study. In their study, they outline the main methodologies discussed by literature for ensuring data security within the cloud. However, it was noted that no direct solutions were provided or discussed by this study which address the gap identified, other than the study itself providing further information on cloud computing data security. In an analysis of the other studies identified, it was noted that while all of the studies recognise the need for developing a deeper understanding of the security of cloud computing, they do not directly address the lack of awareness of employees on cloud computing cyber security. By extension, these studies neither provide solutions for improving employees' awareness on the topic. This finding outlines the lack of attention being given to such a gap, leading to the suggestion of further research to be conducted on this topic.

6. Conclusions

This chapter concludes this study by providing a general outline of the findings as well as in providing suggestions for future studies. Therefore, Chapter 6.1 outlines the core limitations of this study. Chapter 6.2 provides a conclusion to this study and, based on the findings, proposes the way forward for future research.

6.1. Limitations of this study

While a systematic approach was taken to ensure the validity of this study, no single study is perfect and it should be outlined how this study is not without limitations. This chapter discusses the limitations faced by this study.

Firstly, it should be noted that although this research provides an overview of cyber security and cloud computing, it only considers their interconnected relationship. As such, this research fails to fully represent these topics independently. This may inherently result in the study to overlook certain gaps which are inherent to one topic or the other, which could also be of significant importance to the future of that topic. Furthermore, one of this study's findings revolved around the inter-connectedness of different emerging technologies. This study is limited to cloud computing cyber security and so, there may be other cyber security issues which are mainly relevant to other emerging technologies, but which influence all emerging technologies including cloud computing. Given the constraints of this research, such issues would not have been identified.

This research analyses research papers taken from the Google Scholar and Scopus databases. This means that there may be other relevant studies which were not considered within this

research as they were not made available in the two research databases used for this study. Further to this, the limitations set by the inclusion criteria could have resulted in certain viable studies to be overlooked. Such limitations included that this study only considered literature written in the English language, and which were fully accessible in whole, either through the study being Open Access or through the resources provided by the University of Malta. Another such limitation is that the screening and analyses of the chosen studies were conducted by only one person. While measures were taken to mitigate this limitation, as outlined in chapter 3, this could have hindered the objectivity of the results achieved as it is still possible that subjective biases affected the choosing and/or analyses of the studies that were included in the study.

6.2. Concluding Remarks and Recommendations for Future Investigations

Cloud computing's rapidly evolving nature demands great understanding of the technology by industry practitioners. This study addresses the need for enhancing the knowledge on cloud computing by delving into the cybersecurity gaps which require attention by future research. Through the answering of the two research questions set by this study, a total of nine such research gaps were outlined. Firstly, we have seen how the evolving nature of cloud computing cybersecurity issues require people to develop a deeper understanding of these risks. This research also outlines the need for future research to develop better cyber risk management tools, as well as frameworks and regulatory standards which are tailor made to address organisations' cloud computing cyber security needs. Cryptographic algorithms were a key topic discussed by numerous academics who coherently displayed the view that further research should be dedicated to improving such a technology, namely through the further development of genetic and DNA cryptography, and its applicability to enhancing cloud computing cyber security. On top of this, cloud computing infrastructures also require further improvements and optimisation in order to increase efficiency, security, and sustainability of this technology. Such improvements and further research also tie in to the increasing integration between cloud

computing and various other emerging technologies. As such, future research should also address this integration and the various changes it brings to the technology and cyber security industries. We have also seen how the applicability of cloud computing is very wide, and its application to Battery Management Systems is also a topic that requires further research. Finally, this research identified a gap in literature pertaining to the lack of employees' awareness on cloud computing cyber security. As such, it is recommended that future studies should be made to address this gap, ideally through the development of tools and frameworks which organisations may use to educate their employees and ensure that they are aware of the state-of-the-art cloud computing cyber security requirements and standards.

Cloud computing is a vast technology with numerous applications that span over a wide range of industries. Given such vast applicability, it is crucial to ensure that the use of such a technology is done in a secure manner. This ensures the preservation of economies, as well as the safety and privacy of individuals on a global scale.

References

ALQAHTANI, K.S., ALBALAWI, A.M. and FRIKHA, M., 2023. Reviewing of Cybersecurity Threats, Attacks, and Mitigation Techniques in Cloud Computing Environment. *Journal of Theoretical and Applied Information Technology,* **101**(6),.

AMAZON WEB SERVICES, 2023-last update, What is cloud computing?. Available: https://aws.amazon.com/what-is-cloud-computing/ [06/05/, 2023].

AMAZON WEB SERVICES, (., 2023-last update, Runtime security. Available: https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/security-runtime.html2023].

ASLAN, Ö, AKTUĞ, S.S., OZKAN-OKAY, M., YILMAZ, A.A. and AKIN, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics,* **12**(6), pp. 1333.

AVI NETWORKS, 2023-last update, Microservices And Containers . Available: https://avinetworks.com/what-are-microservices-and-containers/2023].

BELL, S. and PARTNER, M., 2017. Cybersecurity is not just a 'big business' issue.

BELL, S. and PARTNER, M., Cybersecurity is not just a 'big business' issue.

CAN, O., THABIT, F., ALJAHDALI, A.O., AL-HOMDY, S. and ALKHZAIMI, H.A., 2023. A Comprehensive Literature of Genetics Cryptographic Algorithms for Data Security in Cloud Computing. *Cybernetics and Systems,* , pp. 1-35.

CLAUSMEIER, D., 2023a. Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review,* **4**(1), pp. 79-90.

CLAUSMEIER, D., 2023b. Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review,* **4**(1), pp. 79-90.

CLOUDFLARE, 2023-last update, What is serverless computing? | Serverless definition. Available: https://www.cloudflare.com/learning/serverless/what-is-serverless/2023].

CRAIGEN, D., DIAKUN-THIBAULT, N. and PURSE, R., 2014. Defining cybersecurity. *Technology Innovation Management Review,* **4**(10),.

CSA, 2023-last update, The Definition of Cloud Computing | CSA. Available: https://cloudsecurityalliance.org/blog/2015/10/26/the-definition-of-cloud-computing/ [06/05/, 2023].

DENG, M.I., KHAN, Z., CHOWDHURY, M. and SHUE, M., 2022. A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications.

EUROPEAN PARLIAMENT, 2023a. The NIS2 Directive: A high common level of cybersecurity in the EU.

EUROPEAN PARLIAMENT, 2023b-last update, What is artificial intelligence and how is it used?.
Available: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used?at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=DSA&at_goal=TR_G&at_audience=&at_topic=Artificial_Intelligence&gclid=Cj0KCQjw6KunBhDxARIsAKFUGs-AKqF9P_pFcrMX6d4qXjnRzoeQBMplOLqQRaxAXsGesc3UX-JcYLgaAh44EALw_wcB2023].

EUROPEAN PARLIAMENT, 10-11-, 2022-last update, Fighting cybercrime: new EU cybersecurity laws explained | News | European Parliament.
Available: https://www.europarl.europa.eu/news/en/headlines/security/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained [Aug 13, 2023].

EUROPEAN PARLIAMENT, Apr 22, 2021-last update, Shaping the digital transformation: EU strategy explained.
Available: https://www.europarl.europa.eu/news/en/headlines/society/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained [13/08/, 2023].

EUROPEAN SECURITIES AND MARKETS AUTHORITY, (., 2023. ESAs consult on the first batch of DORA policy products.

FLORAKIS, C., LOUCA, C., MICHAELY, R. and WEBER, M., 2020. Cybersecurity Risk.

GANNE, A., 2022. Emerging Business Trends in Cloud Computing. *International Research Journal of Modernization in Engineering Technology,* **4**(12),.

GARCIA-PEREZ, A., CEGARRA-NAVARRO, J.G., SALLOS, M.P., MARTINEZ-CARO, E. and CHINNASWAMY, A., 2023. Resilience in healthcare systems: Cyber security and digital transformation. *Technovation,* **121**, pp. 102583.

GOOGLE CLOUD, 2023-last update, What is a cloud service provider?.
Available: https://cloud.google.com/learn/what-is-a-cloud-service-provider#:~:text=A%20cloud%20service%20provider%2C%20or,or%20applications%20over%20the%20internet.2023].

GUO, J. and GUO, H., 2023. Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. *Symmetry,* **15**(5), pp. 988.

HASAN, M.Z., HUSSAIN, M.Z., ALAM, I., SARWAR, N., QURESHI, A.M. and IRSHAD, A., 2023. Impact of Cybercrime on Enterprises in Cloud Computing Environment: A Review, *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)*, 09-11 January 2023 2023, IEEE, pp. 1-6.

HEPFER, M. and POWELL, T.C., 2020. Make cybersecurity a strategic asset. *MIT Sloan Management Review,* **62**(1), pp. 13-18.

HERNANDEZ, A. and KARAHAN, S., 2022. what are the emerging and future technologies that we will have to worry the most about from a security perspective? .

IBM, 2023-last update, What is cloud computing? | IBM.
Available: https://www.ibm.com/topics/cloud-computing [06/05/, 2023].

JHA, R., KUMARI, N. and OMERIBE, C.C., 2023. Cloud Privacy and Security-A Review Paper. *Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596,* **8**(si7), pp. 333-351.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES, 2023. Digital Operational Resilience Act (DORA): public consultation on the first batch of policy products.

KASPERSKY, 2023-last update, What is a Zero-day Attack? - Definition and Explanation . Available: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit2023].

KAUR, R., GABRIJELČIČ, D. and KLOBUČAR, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion,* , pp. 101804.

KHAN, S., KHAN, S. and GALIBEEN, S., 2011. Cloud computing an emerging technology: Changing ways of libraries collaboration. *International Research: Journal of library and Information science,* **1**(2),.

KIMANI KENNETH, ODUOL VITALICE and LANGAT KIBET, 2019. Cyber security challenges for IoT-based smart grid networks.

KOMAR, R. and PATIL, 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),.

KUMAR, R., KATHURIA, S., MALHOLTRA, R.K., KUMAR, A., GEHLOT, A. and JOSHI, K., 2023. Role of Cloud Computing in Goods and Services Tax (GST) and Future Application, *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* 2023, IEEE, pp. 1443-1447.

KWAO DAWSON, J., TWUM, F., HAYFRON ACQUAH, J.B. and MISSAH, Y.M., 2023a. PRISMA Archetype-Based Systematic Literature Review of Security Algorithms in the Cloud. *Security and Communication Networks,* **2023**.

KWAO DAWSON, J., TWUM, F., HAYFRON ACQUAH, J.B. and MISSAH, Y.M., 2023b. RECONNOITERING SECURITY ALGORITHMS PERFORMANCE IN THE CLOUD: SYSTEMATIC LITERATURE REVIEW BASED ON THE PRISMA ARCHETYPE. *Journal of Theoretical and Applied Information Technology,* **101**(6),.

MELL PETER and GRANCE TIMOTHY, 2011. The NIST Definition of Cloud Computing.

MICROSOFT, 2023-last update, What is cloud computing?. Available: https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-cloud-computing#:~:text=Simply%20put%2C%20cloud%20computing%20is,resources%2C%20and%20economies%20of%20scale. [09/07/, 2023].

MIJWIL, M., FILALI, Y., ALJANABI, M., BOUNABI, M. and AL-SHAHWANI, H., 2023. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian journal of cybersecurity,* **2023**, pp. 1-6.

MIJWIL, M., UNOGWU, O.J., FILALI, Y., BALA, I. and AL-SHAHWANI, H., 2023. Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian journal of cybersecurity,* **2023**, pp. 57-63.

MINNA, F. and MASSACCI, F., 2023. SoK: run-time security for cloud microservices. Are we there yet?. *Computers & Security,* , pp. 103119.

NASERI, F., KAZEMI, Z., LARSEN, P.G., AREFI, M.M. and SCHALTZ, E., 2023. Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects. *Batteries,* **9**(7), pp. 382.

NEUMANNOVÁ, A., BERNROIDER, E.W. and ELSHUBER, C., 2022. The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review, *European, Mediterranean, and Middle Eastern Conference on Information Systems* 2022, Springer, pp. 570-585.

NIGHTINGALE, A., 2009. A guide to systematic literature reviews. *Surgery (Oxford),* **27**(9), pp. 381-384.

NIST COMPUTER SECURITY RESOURCE CENTRE, 2023-last update, cybersecurity - Glossary | CSRC. Available: https://csrc.nist.gov/glossary/term/cybersecurity2023].

NOBANEE, H., ALODAT, A., BAJODAH, R., AL-ALI, M. and AL DARMAKI, A., 2023. Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime,* .

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. and BRENNAN, S.E., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *International journal of surgery,* **88**, pp. 105906.

PAGE, M.J., MOHER, D., BOSSUYT, P.M., BOUTRON, I., HOFFMANN, T.C., MULROW, C.D., SHAMSEER, L., TETZLAFF, J.M., AKL, E.A. and BRENNAN, S.E., 2021. PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. *bmj,* **372**.

PAWLICKI, M., PAWLICKA, A., KOZIK, R. and CHORAŚ, M., 2023. The survey and meta-analysis of the attacks, transgressions, countermeasures and security aspects common to the Cloud, Edge and IoT. *Neurocomputing,* , pp. 126533.

RABAI, L.B.A., JOUINI, M., AISSA, A.B. and MILI, A., 2017. A cybersecurity model in cloud computing environments. *Journal of King Saud University-Computer and Information Sciences.* Elsevier, pp. 63-75.

RAHAMAN, M.S., ISLAM, A., CERNY, T. and HUTTON, S., 2023. Static-Analysis-Based Solutions to Security Challenges in Cloud-Native Systems: Systematic Mapping Study. *Sensors,* **23**(4), pp. 1755.

ROTHROCK, R.A., KAPLAN, J. and VAN DER OORD, F., 2018. The board's role in managing cybersecurity risks. *MIT Sloan Management Review,* **59**(2), pp. 12-15.

ROTOLO, D., HICKS, D. and MARTIN, B.R., 2015. What is an emerging technology? *Research Policy,* **44**(10), pp. 1827-1843.

SAEED, S., ALTAMIMI, S.A., ALKAYYAL, N.A., ALSHEHRI, E. and ALABBAD, D.A., 2023. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors,* **23**(15), pp. 6666.

SHAFIQ, M., GU, Z., CHEIKHROUHOU, O., ALHAKAMI, W. and HAMAM, H., 2022. The rise of "Internet of Things": review and open research issues related to detection and prevention of IoT-based security attacks. *Wireless Communications and Mobile Computing,* **2022**, pp. 1-12.

SOVEIZI, N., TURKMEN, F. and KARASTOYANOVA, D., 2023. Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems,* .

SURIANARAYANAN, C. and 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 (IJCAC),* **13**(1), pp. 1-30.

TAHERDOOST, H., 2023. An overview of trends in information systems: emerging technologies that transform the information technology industry. *Cloud Computing and Data Science,* , pp. 1-16.

TAHERDOOST, H., 2021. A review on risk management in information systems: Risk policy, control and fraud detection. *Electronics,* **10**(24), pp. 3065.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2019-last update, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj [Aug 13, 2023].

THE INSTITUTE OF RISK MANAGEMENT, 2014. *Cyber Risk Resources for Practitioners.*

THE INTERNATIONAL BUSINESS MACHINES CORPORATION, (., 2023-last update, What is the internet of things?. Available: https://www.ibm.com/topics/internet-of-things2023].

TOZZI, C., Feb 16, 2022-last update, An intro to cloud-native microservices and how to build them. Available: https://www.techtarget.com/searchapparchitecture/tip/An-intro-to-cloud-native-microservices-and-how-to-build-them#:~:text=Microservices%20are%20a%20core%20component,and%20a%20better%20user%20experience.2023].

VELLELA, S.S., REDDY, B.V., CHAITANYA, K.K. and RAO, M.V., 2023. An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform, *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)* 2023, IEEE, pp. 776-782.

XU, D., 2010. Cloud computing: An emerging technology, *2010 International Conference On Computer Design and Applications* 2010, IEEE, pp. V1-104.