International Journal of Management, Finance and Accounting

A Systematic Review: Risk Management of Cloud Computing Projects in Healthcare

Muhammad Afif Fathullah *[1]
Anusuyah Subbarao[1]
Saravanan Muthaiyah[1]

*Corresponding author afif.fathullah.mmu.edu.my
[1]Faculty of Management, Multimedia University, Cyberjaya, Malaysia

Abstract

Cloud computing has become a major driver for innovation in this technological age. All sectors worldwide have increasingly moved towards cloud adoption, including healthcare. However, cloud computing projects with other IT projects come with risks that could be costly for organizations if they materialized. This study aims to provide an understanding of the risks of cloud computing projects in healthcare by using a systematic literature review augmented by the constant comparison method.63 articles from five major databases written from 2010 to 2022 were reviewed as they are related to cloud computing projects. More specifically, this study shows 198 unique indicators that were categorized into risks, threats, vulnerabilities, probabilities, consequences, and control procedure categories which then were classified into 13 distinct risk classes that can be found in such projects.

Keywords: Cloud Computing, Risk Management, Project Management, Healthcare Risk

Submitted on 21 May 2023; Accepted 20 July 2023; Published on 31 Aug 2023.

This work is licensed under the Creative Commons BY-NC-ND 4.0 International License.

1. Introduction

Cloud computing is a "computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection" (Chan et al., 2012; Grob et al., 2021). It is increasingly perceived as a core driver of business transformation and innovation (Ali et al., 2017) due to its ability to create a competitive environment for businesses to operate without the concern over scale, maintenance and system failure (Singh et al., 2019; Mekawie & Yehia, 2021). In cloud computing, the scale, maintenance and system failure are borne by the cloud computing vendor. These vendors manage their data infrastructure and software; organizations can concentrate on business operations.

However, as with any information technology (IT) architecture project, cloud computing has unique risks and challenges. As such, there is a need for organizations that wish to implement cloud computing to know the risks that may present themselves in the course of the project and how they may control these risks. In all sectors worldwide, cloud computing is being used increasingly. This includes the healthcare sector as it has been stated by Gao and Sunyaev (2019) “that cloud computing possesses unique features such as on-demand self-service and broad network access", which can enhance healthcare organisations by bolstering their current internal health IT strategies.

However, despite all these advantages, cloud computing implementation and adoption are still limited and enveloped by issues in developing countries (Al-Hujran et al., 2018; Mekawie & Yehia, 2021). Multiple risks and challenges affect cloud computing projects that must be faced by the healthcare organization that wishes to adopt cloud computing, such as data leakage, malicious insider threats, insecure API, Denial of Service (DoS), malware injection attacks, and system and application vulnerabilities (Ismagilova et al., 2020).

These risks will not only affect the healthcare organization during the adoption process of cloud computing but also may affect them beyond the adoption. Furthermore, the risks can be costly to a healthcare organization as there can be lost lasting effects in the case of risk actualization such as vendor bankruptcy and non-compliance, security and privacy breach, and staff dissatisfaction and high turn-around.

2. Literature Review

2.1 Cloud Computing Benefits

Scalability, online delivery of software, and virtual services are just advantages of cloud computing (Sultan, 2014). Cloud computing has also shown a positive impact on some organizations by allowing them to have better "cost savings", "improved agility", "enhanced efficiency", "better resource integration", "more business opportunities", and "simplification of complex work resources" (Alghamdi et al., 2021; Mekawie & Yehia, 2021). This is because cloud computing enables businesses to take advantage of current technological innovations such as data analytics and machine learning solutions and established solutions such as "Enterprise Resource Planning (ERP)" online on a scale.

These solutions can be of great benefit to an organization as they can improve the organization's agility, efficiency and more without being burdened with a high cost. Cloud computing gives positive benefits to an organization by having positive impacts on the organization's business by minimizing operating costs and refining the performance of business applications.

Finally, there are several particular benefits of cloud computing in healthcare. [9] stated the benefits were 1) improved patient care; 2) cost saving; 3) energy saving; 4) robust disaster recovery; 5) research; 6) solving the scarcity of resources; 7) rapid deployment; and 8) data availability

2.2 Risk

Risks are traditionally defined as the "possibility of an injury, danger, loss, or other adverse outcomes" and "uncertainty of outcome" (Hampton, 2009; Hopkin, 2017). Besides that, risk has also been viewed not only as a possibility with negative implications but also as a positive one or, in other words, the upside of risk (Hampton, 2009; Hopkin, 2017). However, there is a consensus that no matter whether the risk has a positive or unfavourable implication, they are a combination of both likelihood and consequences (ISO 31000, 2018).

2.2.1 Probability and Consequences

Probability or likelihood is defined as the chance of something happening, whether they are defined, measured, or determined quantitatively or qualitatively (ISO 31000, 2018).

In regards to risk, it constitutes the possibility of the risk materializing. Meanwhile, consequences or impact is defined as the outcome of an event and can be defined, measured, or determined quantitatively or qualitatively (ISO 31000, 2018). In regards to risk, it constitutes the ramifications or outcome if the threat materializes. As such, it can be said that "Risk = Probability/Likelihood X Consequences".

2.2.2 Threat and Vulnerability

Threat and vulnerability are extra important attributes that are related to risk. The reason is that they are related to risk probability, as it has been stated by Kuzminykh (2021) that "Probability = Threat X Vulnerability". Information security threats could be regarded as a potential opportunity to disrupt information security (Kuzminykh, 2021). In a cloud computing environment, threats are opportunities for outside forces to disrupt the organization or their cloud service provider (CSP) information security.

Similarly, vulnerability is internal negative attributes that an organization or its CSP may have such as defects or weaknesses. These vulnerabilities could compromise the organization's cloud confidentiality, integrity, or availability. In a cloud computing environment, attackers use an organisation's or their CSP's inherent cloud vulnerabilities to actualize the threats that will disrupt their information security.

2.2.3 Control Procedures

Control procedures are a measure that maintains and modifies risk (ISO 31000, 2018). The purpose of control procedures is to ensure that an asset is protected and, in turn, maximize its reliability (Hopkin, 2017). There are three different categories of control which are 1) preventive control – controls where risks are eliminated or prevented from happening; 2) detective control – controls that are deployed when organizations wish to discover what are the causes of risks that have already materialized; and 3) corrective controls – controls deployed to rectify and correct risks that have already materialized (Hopkin, 2017).

It was also stated by Landoll (2021) that preventive control allows for the decrease of risk by reducing or eliminating the likelihood of the risk happening, while detective and corrective control allows for risk reduction by reducing the consequences of risk. As the likelihood of risk is derived from threats and vulnerabilities, preventive

control is a control procedure in which threats and vulnerabilities are reduced or eliminated, reducing the likelihood of risk materializing.

3. Research Methodology

The research method selected for this study is Systematic Literature Review (SLR) in conjunction with the Constant Comparison Method (CCM) has been chosen as the research method for this paper. This paper follows the SLR methodology provided by (Kitchenham, 2016). Landoll (2021) has shown that SLR consists of three phases which are 1) Planning Review, 2) Conducting Review, and 3) Documenting Review, with each phase having different activities. Meanwhile, CCM has been stated by Onwuegbuzie (2012) to be a qualitative analysis technique for reviewing the literature. There are three stages in CCM 1) Open Coding, 2) Axial Coding, and 3) Selective Coding. This paper will focus on presenting the activities and steps in the planning review and conducting review phases. Figure 3.1 shows the activities done throughout these three phases and how it was used in conjunction with CCM, along with the time taken to complete each activity.

Several steps were taken to define the search protocol, which were 1) Define the SLR research question; 2) Search strategy; 3) Study selection; and 4) Inclusion and exclusion criteria. The protocol was then validated by two other researchers to ensure validity.

Research questions were designed to identify the prevalent risks and related challenges along with related indicators in cloud computing projects in healthcare. Firstly, the prevalent risk in cloud computing projects is examined to determine the likelihood and consequences in the healthcare industry. As such, the research questions for this study are as follows:

RQ1: What are the prevalent risks in cloud computing projects in healthcare?

RQ2: What are the challenges related to the risks of cloud computing projects in healthcare?

RQ3: What are the effects of risks in cloud computing projects in healthcare?

RQ4: What are the solutions for risks in cloud computing projects in healthcare?

Earlier studies between 2006 and 2010 described cloud computing as an improved model of delivering computing resources (Kuo, 2011; Chan et al., 2012). As such, the cloud computing trend gained momentum in 2010. The specific timeline for the study selection is January 2010 – January 2022. Furthermore, the papers were also searched from five different digital library databases; forward snowballing was also used in this SLR. The five digital library databases searched from are presented in Figure 1.

Inclusion and exclusion criteria for paper selection were also constructed for this study. Criteria allow for the researcher to initially consider which paper is suitable for this study. The criteria constructed are shown in Figure 3.2

3.2 Conduct Review

The conduct review segment shows the activities and steps operated to systematically review the paper.

3.2.1 Boolean Operator and Phrase Searching

The Boolean operators that are used for the phrase searching in the digital library shown in 3.1.2.3 Study Selection are based on the keywords and synonyms/related keywords shown in 3.1.2.2 Search Strategy. The research phase used for the IEEE, ACM, Springer Link, and Emerald were:

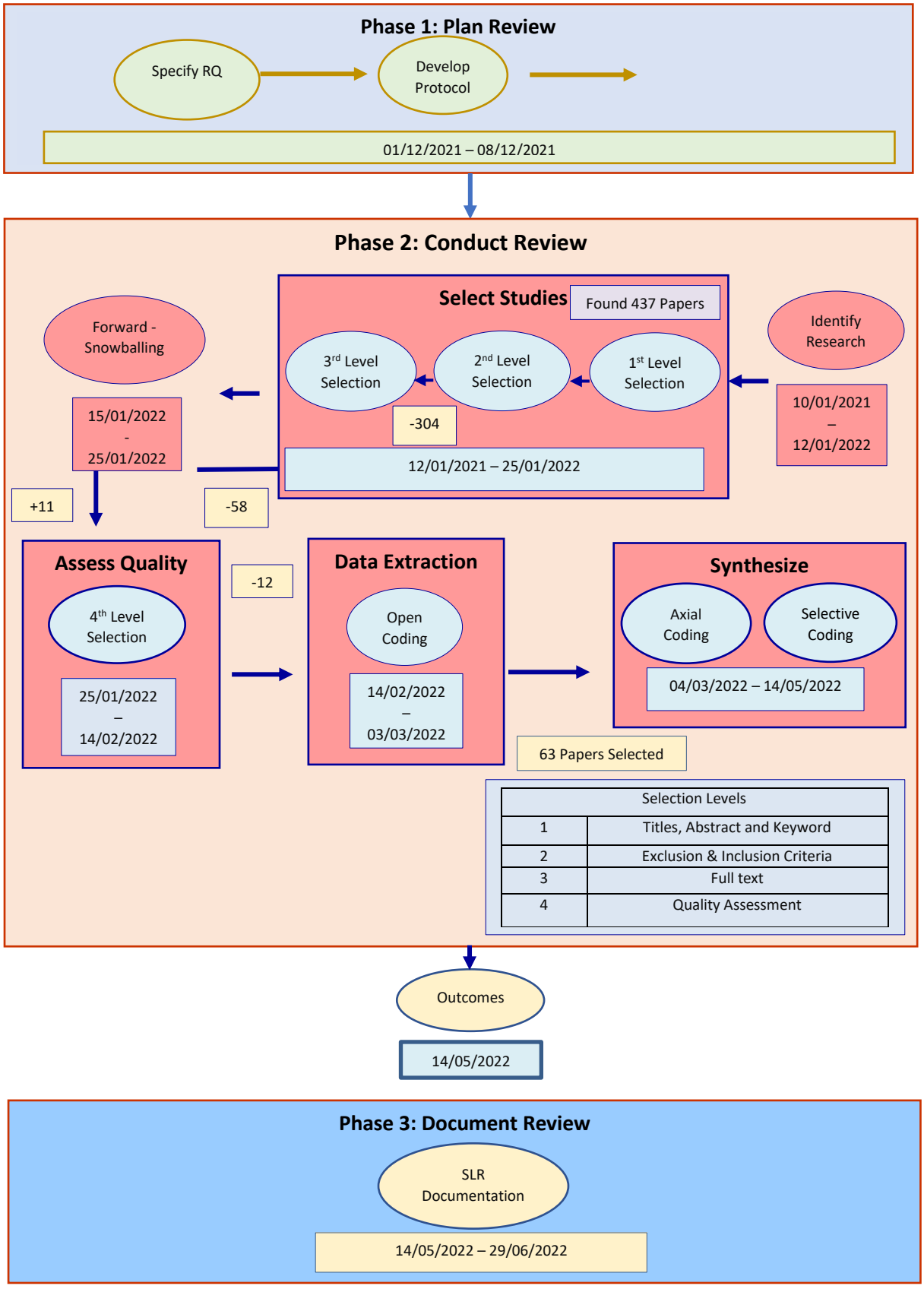
(“Cloud Computing” OR “Fog Computing” OR” Edge Computing” OR “Saas” OR “Paas” OR “Iaas”) AND (“Projects” OR “Strategy” OR “Activity”) AND (“Healthcare” OR “Medical Management”) AND ((“Risk” OR “Exposure” OR “Possibility” OR “Opportunity”) OR (“Challenges” OR “Threat” OR” Obstacles”)).

Meanwhile, the phrase searcher for Science Direct can only use eight Booleans, as such the phrase searching which was used was:

(“Cloud Computing”) AND (“Projects” OR “Strategy”) AND (“Healthcare” OR “Medical Management”) AND ((“Risk” OR “Exposure”) OR (“Challenges”)).

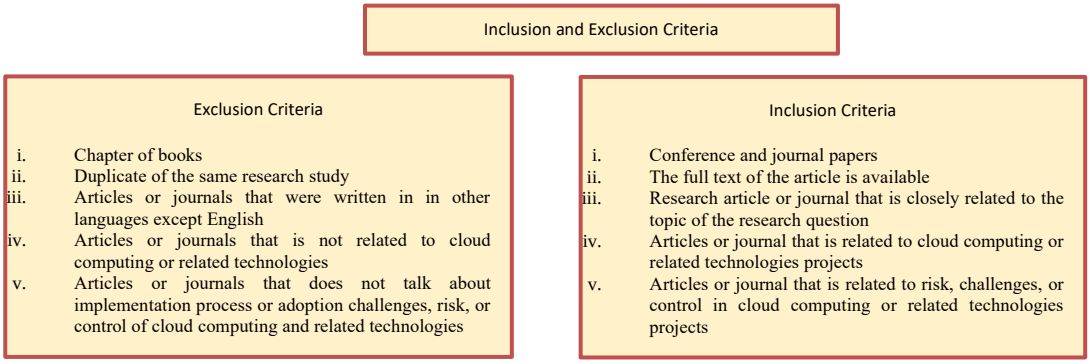
Furthermore, the Springer Link digital library could specify to search in which fields, two fields were chosen. These fields were the discipline of business and management along with the discipline of medicine and public health.

Figure 3.1 SLR and CCM Activities and Timeline



- ACM (https://dl.acm.org/);
- IEEE (https://ieeexplore.ieee.org/Xplore/home.jsp);
- Springer Link (https://link.springer.com/);
- Science Direct (https://www.sciencedirect.com/);
- Emerald (https://www.emerald.com/insight/).

Figure 3.2 Inclusion and Exclusion Criteria



3.2.2 Select Studies and Assess Quality

The studies and papers were selected and asses according to Kitchenham protocol Kitchenham (2016) which serves as the within-study literature analysis phase of this SLR. This protocol shows that there are four levels to selecting academic papers and assessing the quality of the aforementioned papers. The 1st level selection is by the academic paper Title, Abstract, and Keyword; The 2nd level selection is by assessing whether the paper meets the inclusion and exclusion criteria. The 3rd level selection is done by the researcher reading the full text and choosing whether the paper is suitable to gain insight for the SLR goal. The 4th level selection is the quality assessment in which five questions were stated to assess the quality of the paper as shown in Table 3.1. Table 3.2 highlights the selection criteria explained above.

Table 3.1 Quality Assessment Question

No	Question	Answer
1	Are the aims of the research stated clearly?	Yes/No
2	Is the research design clearly specified?	Yes/No/Partially
3	Was the data collection method carried out accordingly?	Yes/No/Partially
4	Has the analysis been done appropriately?	Yes/No/Partially
5	Does the researcher(s) display(s) enough data to support their analysis and conclusion?	Yes/No/Partially
Yes = 1, Partially = 0.5, No = 0 Q1 + Q2 + Q3 + Q4 + Q5 >= 3.5 = Accepted		

Table 3.2 SLR Paper Selection Level

Database/Digital Library	1st Level selection (Titles, abstract, and keyword)	2nd Level selection (Exclusion & Inclusion Criteria)	3rd Level selection (Full text)	4th Level selection (Quality Assessment)
ACM	93	19	10	9
IEEE	49	24	11	9
Science Direct	193	42	23	19
Springer Link	47	11	5	5
Emerald	55	37	15	12
Forward Snowballing	-	-	11	9
Total	**437**	**133**	**75**	**63**

3.2.3 Data Extraction

The data extraction phase for this SLR was done to achieve the research goals of this study. The data extracted from the papers chosen after the 4th selection are called indicators. CCM's first stage which is "open coding" was done in this phase. The indicators were separated into six categorical themes related to risk management which is 1) Risk, 2) Probability, 3) Consequences, 4) Threat, 5) Vulnerability, and 6) Control Procedures. These categories were selected as they relate to the prevalent risk, their related challenges, effects, and control procedures in cloud computing projects in healthcare. Each indicator was given a unique ID based on the categories for the initial identifier with Risk = R, Consequences = C, Probability = P, Threat = T, Vulnerability = V, and Control Procedure = Co. The indicators were also given names with the name of the indicators being based on the names that were given to them by the authors of the

paper and if there were not specifically named by the authors, the names were taken from the explanation provided by the author and written by the researcher.

3.2.4 Data Synthetization

The last activity of the conduct review phase is the data synthetization stage. Several steps were taken using CCM as the reference to synthesize the indicators which were extracted from the papers. The steps taken are stated below:

1)The indicators were separated based on their type which are risk, probability, consequence, threat, and control procedure.

2)The probability, consequences, threat, and control procedure indicators were further separated into which risk relates to them.

3)All of the indicators were grouped by the researcher with other similar meaning indicators of their type which were found through their name and/or the meaning of their explanations of their meaning.

4)The indicators were then consolidated by the researcher and were given new or existing names and explanations of their meaning. The researcher had written the names and meanings through their understanding of what the paper's author had written about the indicators.

5)The consolidated indicators were then given ID based on their risk and when they were constructed.

Steps one to three comprises the "axial coding" stage of the constant comparison method while step four to five comprise the "selective coding" stage.

4. Results

Once the data synthetization has been finalized, this study was able to identify answers to the research questions stated. Thus, the findings of each research question of this study have been obtained. This section represents the findings and discussion section of this study to answer the research questions stated. From the data synthetization finalized, it has been found that the indicators discovered are categorized into nine distinct risk classes as shown in Table 4.1.

Table 4.1 Risk Classes

ID	Risk Class Name
1	Lack of Transparency
2	Reliability and Performance Issues
3	Vendor-Lock In
4	Security and Compliance Issues
5	Cyber Attack
6	Data Leakage
7	Organizational Change
8	CSP Viability
9	Public Perception

4.1 Findings on RQs

This section presents the answers to the RQs based on the indicators extracted and synthesized from the academic papers found.

4.1.1 RQ1: What are the prevalent risks in cloud computing projects in healthcare?

To answer this question and reach our RO1 "identify prevalent risks of cloud computing projects in healthcare", we have looked at the indicators that are under the category theme of "Risk". As a result, we have constructed and discovered 18 unique risk indicators with each relating to one risk class as shown in Table 4.2 We have also shown the number of academic papers used to synthesize the risk indicator and which paper they were from.

Table 4.2 Risk Indicator

Risk Indicator Name	Number of Papers	Study Identifiers	Risk Class								
			1	2	3	4	5	6	7	8	9
Lack of Transparency	4	S10; S23; S28; S63									
Technical Reliability and Performance Issues	5	S7; S18; S26; S44; S62									
Availability and Flexibility	9	S12; S23; S24; S30; S32; S43; S34; S46; S48									
Quality of Service (QoS)	2	S39; S56									
Vendor-Lock In and Lack of Application Portability and Interoperability	13	S10; S14; S20; S23; S32; S38; S41; S43; S46; S48; S52; S53; S60									
Interoperability, Integration, and Transition	4	S23; S32; S33; S41									

Risk Indicator Name	Number of Papers	Study Identifiers	Risk Class								
			1	2	3	4	5	6	7	8	9
Error in Choosing CSPs	1	S34									
Data Security	27	S3; S4; S6; S7; S10; S12; S14; S16; S17; S19; S21; S22; S23; S27; S28; S29; S35; S39; S41; S44; S47; S48; S51; S55; S58; S60; S63									
Security and Compliance	15	S1; S2; S9; S10; S11; S12; S18; S20; S23; S32; S33; S34; S38; S43; S48									
Security and Privacy	22	S8; S15; S24; S25; S26; S29; S30; S31; S32; S34; S36; S37; S40; S42; S45; S46; S52; S53; S54; S55; S57; S59									
Cyber Attack	10	S5; S6; S18; S25; S29; S34; S41; S48; S53; S61									
Data Leakage	5	S1; S4; S5; S10; S50									
Data Leakage and Privacy	4	S13; S19; S23; S49									
Usurpation of Identity and Unauthorized Access	1	S60									
IT Organizational Change and Capability	3	S12; S24; S43									
Organizational Change and Management Failure	2	S34; S55									
CSPs Viability	4	S25; S48; S60; S61									
Public Perception, Usability, and End users Experience	2	S11; S55									

4.1.2 RQ2: What are the challenges related to the risks of cloud computing projects in healthcare?

To answer this question and reach our RO2 “identify challenges related to risks of cloud computing projects in healthcare”, we have looked at the categories theme of “Threats”, “Vulnerability”, and “Probability". This is because these categories are affecting the risk Hopkin (2017) and as such can be implied to be their related challenges. As a result, we have constructed and discovered several indicators relating to these categories.

4.1.2.1 Threat Indicators

Through data synthetization of indicators under the category theme of "Threat", we were able to construct and discover 26 unique threat indicators relating to risk classes three, four, five, six, and eight as can be seen in Table 4.3.

Table 4.3 Threat Indicator

Threat Indicator Name	Number of Papers	Study Identifiers	Risk Class				
			3	4	5	6	8
The use of Data Except Perimeter	1	S60	■				
Lack of Technical Standards	1	S53	■				
Abuse of Cloud Resources	2	S4; S6		■	■		
Data and Service (Un)Availability	4	S31; S45; S53; S55		■			
(Distributed) Denial of Service Attack (DDoS/DoS)	3	S4; S17; S18		■	■		
Loss of Data	3	S6; S55; S60		■	■		
Scalability	5	S18; S35; S45; S54; S55		■			
Data Privacy	5	S9; S15; S25; S30; S31		■			
Data Breach and Loss/Leakage	6	S4; S6; S17; S36; S43; S55		■			
Cyber Attack	1	S59		■			
Energy and Resource Depletion Threats	1	S18		■			
Flexibility	1	S55		■			
Natural Hazard	1	S27		■			
Phishing/Masquerading/ Imposter Threats and Integrity Violations	1	S18		■			
Third-Party Entry Software	1	S27		■			
Transfer Data Between Countries	1	S10		■			
Wrong Application of Cloud Service	1	S31		■			
Data Confidentiality and Integrity	2	S29; S53			■		
Privacy Breaches	1	S25			■		
Data Ownership	1	S29			■		
System Hack	1	S25			■		
Hypervisor and Rootkit Attack	1	S5			■		
Data Integrity	1	S49				■	
ARP Poisoning	1	S5				■	
VM Backdoors	1	S5				■	
Cessation of Service	1	S60					■

4.1.2.2 Vulnerability Indicators

Through data synthetization of indicators under the category theme of "Vulnerability", we were able to construct and discover 26 unique vulnerability indicators relating to risk classes two, three, four, five, six, seven, and eight as can be seen in Table 4.4.

Table 4.4 Vulnerability Indicators

Vulnerability Indicator Name	Number of Papers	Study Identifiers	Risk Class						
			2	3	4	5	6	7	8
Overcrowding	1	S25	■						
Data Centres	1	S18	■						
Insecure Interfaces and APIs	1	S4	■		■				
Difficulty to Negotiate SLA	1	S10		■					
Management of Cloud by Incompetent or Malicious People	1	S60		■					
Non-compliance with Security Requirements	1	S60		■					
Insufficient Due Diligence	2	S4; S6			■	■			
Malicious Insiders	8	S4; S6; S19; S27; S30; S31; S43; S59			■	■	■	■	
Shared Technology Issues	4	S4; S6; S31; S35			■	■	■		
Data Confidentiality and Integrity (Modification)	7	S16; S17; S23; S29; S37; S45; S60			■				
Weak Access Control and User Authentication	7	S4; S5; S17; S29; S31; S48; S60			■	■	■		
Lack of Standardization and Compatibility /Interoperability	6	S18; S35; S36; S45; S53; S55			■				
Data Location and Ownership	3	S23; S29; S45			■				
Flawed Hypervisor	4	S18; S23; S45; S48			■				
Loss of Control over Data in the Cloud	2	S10; S60			■				
Additional Training for Cloud	1	S53			■				
System Security Vulnerability	1	S31			■				
Unsecure Network	1	S27			■				
Virtualization Security	1	S31			■				
Integration Complexity	1	S53				■			
Cloud Storage	1	S61				■			
Transfer Data Between Countries	1	S10					■		

Vulnerability Indicator Name	Number of Papers	Study Identifiers	Risk Class						
			2	3	4	5	6	7	8
Lack of Trust with CSPs	1	S49							
Moving to Another Supplier	1	S60							
End of Contract	1	S61							
Cloud Storage	1	S60							

4.1.2.3 Probability Indicators

Through data synthetization of the indicators under the category theme of "Probability", we were able to construct and discover 51 unique probability indicators relating to risk classes one, two, three, four, five, six, and seven as can be seen in Table 4.5.

Table 4.5 Probabilities Indicators

Probability Indicator Name	Number of Papers	Study Identifiers	**Risk Classes**						
			1	**2**	**3**	**4**	**5**	**6**	**7**
Audit Limitation	1	S4							
SLAs Clause	1	S4							
Operating System Vulnerability	1	S4							
Cloud Spend	1	S62							
Complexity and Lack of Expertise in Cloud Computing	1	S62							
Organization Governance	1	S62							
Poor Internet/ Broadband Infrastructure	3	S24; S25; S46							
Security of Interface and APIs	2	S4; S62							
Scalability	1	S25							
Exit Clause	1	S43							
Legal Implications	1	S43							
Organization EA and IT Maturity	1	S23							
Lack of Interoperability and Portability of CSPs	1	S52							
Lack of Experts	1	S53							
Mal-configuration of AAA Services	1	S4							
Lack of Security System Awareness	1	S4							
Malicious Insiders	1	S4							
Internet Dependency	1	S4							
Insecure Interface and APIs in regards to AAA	1	S4							
Data Security Protection Policies	2	S4; S29							
Effective Communication	2	S43; S48							
Lack of Knowledge and Information, Experts, and Skills	4	S2; S26; S48; S53							
Uncontrolled Rollback	1	S4							
Lack of Technical Knowledge	2	S6; S22							
Cloud Cartography	1	S4							
CSP Integrity and Capability	1	S19							
Data not Encrypted	1	S4							
Incomplete Data Deletion	1	S4							
Uncontrolled Migration	1	S4							
Vulnerabilities in Virtual Network	1	S4							
Platform and Software Security	1	S25							

Probability Indicator Name	Number of Papers	Study Identifiers	Risk Classes						
			1	2	3	4	5	6	7
Lack of IT Policies	1	S12							
Limited Information on Compliance	1	S12							
Trust and Privacy Requirement	2	S4; S30							
High Demand of Patient Data	1	S4							
Weak AAA Mechanism	2	S4; S5							
Lack Of Security, Resources and Expertise	2	S1; S5							
Failure to Observe Required Safeguards	1	S1							
Organization Personnel Account Usage	1	S2							
Data Protection and Portability	1	S4							
AAA Vulnerabilities	1	S4							
Capability of Virtual Machines (VMs) to be Copied	1	S4							
Transparency of Data for Users	1	S4							
Poor Patch Management	1	S4							
Poor Provider Selection	2	S4; S19							
Correlation between SLAs, Privacy Requirement, and Data Breaches	1	S49							
Internal Control and HR Policies	1	S49							
Lack of Understanding of Cloud Technology and Privacy Risk	1	S49							
Access to Computing Technologies	1	S24							
Human Resource Capability	1	S12							
IT Staff Limited Experience in Cloud	1	S12							

4.1.3 RQ3: What are the effects of risks in cloud computing projects in healthcare?

To answer this question and reach our RO 3 "Identify effects of risks in cloud computing projects in healthcare", we have looked at indicators under the category theme of "Consequences". These consequences of risk have been described as the effect of risk and what happens if a risk materialized (Hopkin, 2017). After that, through data synthetization, we were able to construct and discover 31 unique consequences indicators as can be seen in Table 4.6.

Table 4.6 Consequences Indicators

Consequences Indicators Name	Number of Papers	Study Identifiers	Risk Class								
			1	2	3	4	5	6	7	8	9
Expectation Management	1	S28									
Loss of Healthcare Facility Reputation including Trust of Patient	1	S4									
Loss of Personal and Organization Data	2	S4; S6									
Interference with Medical Equipment	1	S25									
Loss of Data Availability and Recoverability	2	S30; S48									
Loss of Life	1	S23									
High Latency	1	S39									
Accountability	1	S25									
Lower QoS	1	S52									
Loss of Data Availability and Recoverability	1	S48									
Loss of Service Delivery and Compromised	1	S4									

Consequences Indicators Name	Number of Papers	Study Identifiers	Risk Class								
			1	2	3	4	5	6	7	8	9
Network											
Loss of Healthcare Staff Loyalty and Experience	1	S4									
Loss of Intellectual Property	1	S4									
Failure of Physical Hardware	1	S4									
Data Breach during Migration	1	S28									
Loss of Data Confidentiality and Privacy	3	S9; S21; S30									
Loss of Data Integrity	1	S21									
Data Modified	1	S59									
Data Security	1	S20									
Incompatibility with Values	1	S12									
Poor Encryption Key Management	1	S11									
Privilege Abuse and Misuse of Health Records	2	S11; S29									
Security Breaches Cost/Expenses	1	S30									
Comprise Cloud Database Architecture	1	S5									
Negative Impact to Patient	1	S5									
SLAs Void	1	S41									
Loss of Personal Data	1	S4									
Exposure of Patient Privacy and Confidentiality	1	S1									
Loss of Healthcare Facility Reputation, Credibility and Trust	2	S4; S49									
Exposure of Patient Privacy and Confidentiality	1	S1									
Data Transfer Ability	1	S25									
Lack of Trust	1	S11									

4.1.4 RQ4: What are the solutions for risks in cloud computing projects in healthcare?

To answer this question and reach our RO4 “Identify solutions for risks of cloud computing projects in healthcare”, we have looked at indicators under the category theme of “Control Procedures”. Control procedures are seen as measures that can act as solutions for risks (Hopkin, 2017; Sookhak et al., 2021). After that, through data synthetization, we were able to construct and discover 45 control procedure indicators as can be seen in Table 4.7.

Table 4.7 Control Procedure Indicator

Control Procedures Indicator Name	Number of Papers	Study Identifiers	Risk Classes								
			1	2	3	4	5	6	7	8	9
Clients Clarification	1	S23									
Risk Assessment and Accountability of CSPs	2	S2; S4									
Privacy Policy	1	S2									
Cloud Audit	7	S1; S2; S23; S43; S48; S52; S63									
Data Backups, Storage, and Processing	2	S39; S48									

Control Procedures Indicator Name	Number of Papers	Study Identifiers	Risk Classes								
			1	2	3	4	5	6	7	8	9
Careful Vendor Selection/Due Diligence	1	S48		■							
Due Diligence on SLA	4	S12; S32; S48; S56		■							
OWASP	1	S4		■		■					
Physical Administrative and Security Control	2	S39; S48		■		■	■				
Cloud Monitoring Tools	2	S25; S48		■		■	■				
Risk Assessment	1	S48		■	■	■					
Defined Matrixes	1	S14			■						
Open Consent Standards	1	S32			■						
Account Registration and Validation	1	S4				■	■	■	■		
SLAs	4	S4; S10; S14; S48				■		■			
Securing Hypervisor	1	S4				■					
Storage and Processing	1	S39				■					
Data Encryption	10	S4; S5; S15; S16; S23; S30; S31; S40; S48; S49				■	■	■			
Access Control	4	S4; S27; S37; S59				■		■	■		
Blockchain	2	S17; S37				■					
Consult with IS Experts	1	S22				■					
Due Diligence on Security and its SLAs	2	S23; S31				■					
Group Key Management	1	S59				■					
Host Data Inside Country	1	S32				■					
Investment on Effective Security Policy	6	S5; S27; S31; S32; S43; S58				■		■			
Maturity Model for Healthcare Cloud Security (M2HCS)	1	S51				■					
Privacy Aware Reversible Watermarking as Digital Signature	2	S4; S57				■					
Secure Data Storage on External Media	1	S27				■					
Secure use of Internet and Email	1	S27				■					
Staff IT Training	2	S27; S36				■					
Standardization and Synchronization of protocols	1	S36				■					
Transparency in Processes and Teams	1	S36				■					
Understanding the Downside of Risk	1	S38				■					
Properties Isolation	1	S4				■	■				
BFT (Byzantine Fault Tolerance)	1	S21				■					
Public Blacklist Enforcement	1	S4					■				
AAA Mechanism	1	S5					■				
Proper Security Configuration	2	S4; S5					■				
Appointing Data Custodian and Accountability	2	S13; S49						■			
Limiting Physical Access	1	S49						■			
Privacy Strategy	1	S49						■			
Segregation of Data	2	S49; S60						■			
Change Management Team	1	S12							■		
Accountability of CSPs	1	S2								■	

5. Discussion

This section presents the discussion of this SLR study. The discussion for this study is separated into four parts for each RQ.

5.1 Discussion on RQ1

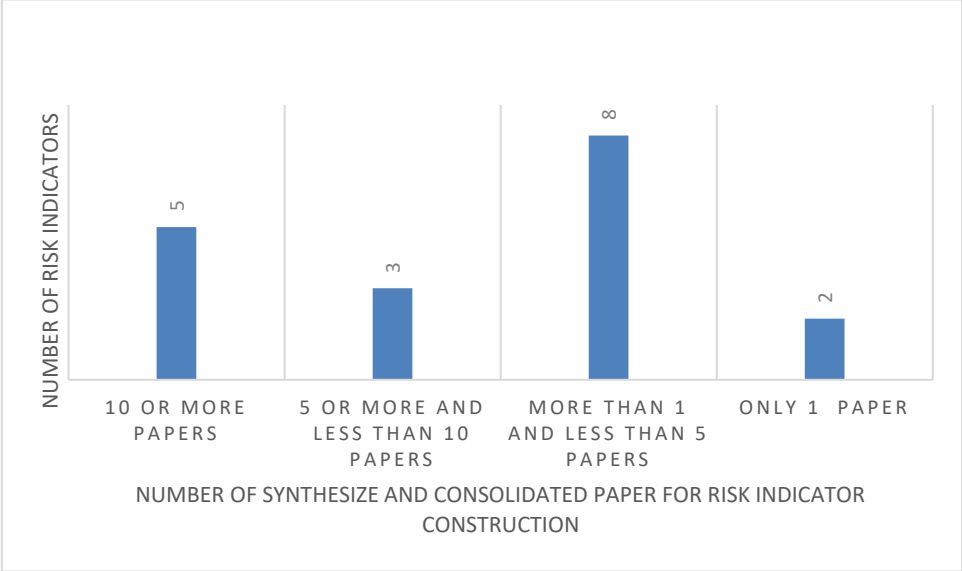
This section presents a discussion of the findings of RQ1. As such, this section will discuss the indicators found in the category theme of "Risk" because they are the prevalent risks of cloud computing projects. The risk indicators were constructed based on the number of papers shown in Figure 5.1.

5.2 Discussion on RQ2

This section discusses the results of RQ2 which are on the three indicators category of "Threat", "Vulnerability", and "Probability". From the aforementioned categories discovered, several interesting facts were found. The first is, that it was discovered that even though data breach/leakage and cyber-attack are risk indicators in their own right, they are also considered threat indicators for the risks in the risk class of security and compliance issues. S59 has stated that cyber-attacks could lead to security and privacy issues if the attack is not contained. Meanwhile, S17 has stated that data breaches/leakage disrupts cloud computing security and can cause compliance and privacy issues.

The next interesting fact that was found is that there are threat and vulnerability indicators that were considered as probability indicators risks in cloud computing projects in healthcare. The threat indicator that was also considered as a probability indicator is scalability. Scalability is considered a threat for risk class four while it was considered a probability for risk class two. S18 stated that "the lack of or low scalability can cause security and compliance" issues while S25 states that scalability of cloud computing that is not clearly defined by an organization during the adoption process can cause reliability and performance issues after its adoption.

Figure 5.1 Number of risk indicators divided by how many papers were discussing them



The vulnerability indicator that is also considered a probability indicator is malicious insiders. Malicious insiders are stated by S4 to be an organization's vulnerability that is related to security and compliance issues, as insiders are organization staff, employee, partner, etc. such existence of such insiders are an organization's internal weakness. However, S4 also states that the existence of malicious insiders in an organization can cause the risk of security and compliance issues to arise. This shows that there is a relationship between vulnerability and threat towards probability as they can affect the probability of the risk happening as stated by [13]. Based on these facts it can be seen that some risks of cloud computing projects in healthcare could be interrelated with each other and not necessarily independent. Furthermore, challenges related to risks of cloud computing projects in healthcare can be similar and reciprocal to each other.

5.3 Discussion on RQ3

This section discusses the results of RQ3 which are indicators in the category of "Consequence". From the consequence indicators discovered, it was found that loss of healthcare facility reputation including the trust of the patient is an effect of materialization of risks belonging to reliability and performance issues, security and compliance issues, cyber-attack, and organizational change risk classes. It was stated by S4 that if risk indicators in the aforementioned risk classes materialized it will impact the

healthcare facility's reputation negatively which can cause patients to lose trust in the facility. From this, it shows that a healthcare organization's reputation and the trust of its patients can be lost if a risk materializes.

Besides that, the most discussed consequence of risks materializing is loss of data confidentiality and privacy which is an effect of risks in the risk class of security and compliance issues materializing. It was stated by S30 that failure to provide adequate security on a cloud computing architecture in the healthcare sector can lead to the loss of data confidentiality and privacy. The loss of confidentiality and privacy can happen to both organization and client data as stated by S9 and S21. These discussions show that the effect of cloud computing risk materializing can have devastating consequences to an organization not only internally but also externally.

5.4 Discussion on RQ4

This section discusses the result of RQ4 which are indicators category of "Control Procedures". The results show that cloud audit could be a control procedure for most risk classes. As it can be a control procedure for risks belonging to five risk classes which are lack of transparency, security and compliance issues, cyber-attack, data leakage, organizational change, and public perception.

S52 mentioned that an organization by enforcing cloud audits can increase the level of confidence and trust of cloud consumers and users in the cloud service. S2 stated that audit logs and cloud audits are put into emphasis when it concerns healthcare data. Meanwhile, S63, S52, and S23 stated that enforcing cloud audits can improve security and mitigate security, data breach, and cyber-attack issues as it allows for weaknesses in a cloud computing architecture to be found before exploitation by unauthorized users. However, S48 has stated that the rate of implementation of third-party cloud audits in an organization is low as only 17% of organizations implement them. Besides that, S63 has stated that the onset of quantum computing will make most cloud auditing that uses a public auditing scheme obsolete.

The most discussed control procedure for risks of cloud computing projects in healthcare is encryption as it is said to be a viable control procedure for risks belonging to the security and compliance issues, cyber-attack, and data breach/leakage risk classes. It was also stated by S30 that as a technical safeguard it has increased the protection of

electronic health records. However, it was stated by S23 and S31 that insufficient and inconsistent encryption policies can instead make encryption of data a vulnerability as such it must come hand-in-hand with privacy policy and strategy which are also control procedures discovered in this study. Furthermore, it was also stated by S48 that only 32% of organizations employ data encryption but this may be due to their respondents being users who do not know their data is encrypted in the back-end as such awareness and dissemination of knowledge to users may be vital to ensure protection.

Besides that, S15 and S16 have also stated that new encryption methods such as homomorphic encryption which can realize ciphertext computation and protect outsourced privacy content provide more robust protection for clients and users in a cloud computing environment as it allows for better confidentiality and integrity of data. S49 have stated that older encryption method may not work since the pace of technology is still progressing. However, it was also stated by S16 that the computational power needed to enforce fully homomorphic encryption which may cause the availability of data to be compromised as stated that a partially homomorphic encryption method may be more suitable to be deployed.

This discussion on control procedures has shown that there are viable options to secure a cloud computing project during and after implementation such as cloud audit and encryption. However, it has also shown that control procedures have their weaknesses and sometimes must be deployed concurrently with other control procedures that need to be fully utilized. As such, this shows that while control procedures can control the risks of cloud computing projects in healthcare, they must be deployed strategically and meaningfully by a healthcare organization for their benefits to be fully realized.

6. Conclusion

To conclude, the goal of this study was to identify prevalent risks in cloud computing projects in healthcare along with their challenges, effects, and solutions through SLR. As such we were able to achieve our aim, through the discovery and construction of 198 unique indicators in the category of:

- Risk
- Threat

- Vulnerability
- Probability
- Consequence
- Control Procedure

We believe that the results discovered from our study can help researchers and practitioners interested in knowing about risk management indicators that are prevalent in cloud computing projects in healthcare.

However, we encountered some limitations during our study, firstly they were not a lot of studies on risk management of cloud computing projects in healthcare, so we had to include several papers that discuss the risks of cloud computing projects in other sectors. Secondly, as we only had access to the ACM, IEEE, Science Direct Springer Link, and Emerald databases, we were not able to find papers in other databases such as PubMed, etc.

Moving forward, we will be validating the indicators we have found with experts' participants to determine whether the discovered indicators are substantial enough to construct an artifact for risk management of cloud computing projects in healthcare. We also hope that more research can be done in this field as cloud computing projects are being adopted extensively throughout the whole world due to an organization's interest or government policy. Risk management and decision-making of cloud computing projects are essential in research as it ensures confidentiality, integrity, and availability, especially in the healthcare sector as it involves people's lives and health.

References

Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2018). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017, 2018-Janua, 373–378. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62

Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry. IEEE Access, 6, 19140–19150. https://doi.org/10.1109/ACCESS.2018.2805919

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health Cloud: Opportunities and Challenges. Future Internet, 4(3), 621–645. https://doi.org/10.3390/fi4030621

Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M2HCS). Information and Computer Security, 28(3), 321–345. https://doi.org/10.1108/ICS-05-2019-0060

Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2020). Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics. Annals of Operations Research. https://doi.org/10.1007/s10479-020-03620-w

Alarcon, M. L., Nguyen, M., Debroy, S., Bhamidipati, N. R., Calyam, P., & Mosa, A. (2021). Trust Model for Efficient Honest Broker based Healthcare Data Access and Processing. 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events, PerCom Workshops 2021, 201–206. https://doi.org/10.1109/PerComWorkshops51409.2021.9430954

Aleem, A., & Ryan Sprott, C. (2012). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. Journal of Financial Crime, 20(1), 6–24. https://doi.org/10.1108/13590791311287337

Alghamdi, B., Potter, L. E., & Drew, S. (2021). Validation of architectural requirements for tackling cloud computing barriers: Cloud provider perspective. Procedia Computer Science, 181, 477–486. https://doi.org/10.1016/j.procs.2021.01.193

Alharbi, F., Atkins, A., & Stanier, C. (2017). Cloud computing adoption readiness assessment in saudi healthcare organisations: A strategic view. ACM International Conference Proceeding Series. https://doi.org/10.1145/3018896.3025156

Al-Hujran, O., Al-Lozi, E. M., Al-Debei, M. M., & Maqableh, M. (2018). Challenges of cloud computing adoption from the TOE framework perspective. International Journal of E-Business Research, 14(3), 77–94. https://doi.org/10.4018/IJEBR.2018070105

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43(July), 146–158. https://doi.org/10.1016/j.ijinfomgt.2018.07.009

Ali., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. International Journal of Information Management, 37(6), 639–649. https://doi. org/10.1016/j.ijinfomgt.2017.05.008

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). EHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering, 2019. https://doi.org/10.1155/2019/7516035

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A study of Saudi Public Sector. Procedia Computer Science, 130, 1037–1043. https://doi.org/10.1016/j.procs.2018.04.145

Alzoubi, Y. I., Al-Ahmad, A., & Kahtan, H. (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. Computer Communications, 182(April 2021), 129–152. https://doi.org/10.1016/j.comcom.2021.11.005

Aski, V. J., Dhaka, V. S., Kumar, S., Verma, S., & Rawat, D. B. (2021). Advances on Networked eHealth Information Access and Sharing: Status, Challenges and Prospects. Computer Networks, 204(April 2021), 108687. https://doi.org/10.1016/j.comnet.2021.108687

Belbergui, C., Elkamoun, N., & Hilal, R. (2019). Cloud computing: Overview and risk identification based on classification by type. Lecture Notes in Networks and Systems, 49, 19–34. https://doi.org/10.1007/978-3-319-97719-5_2

Bernsmed, K., Cruzes, D. S., Jaatun, M. G., Haugset, B., & Gjaere, E. A. (2014). Healthcare services in the cloud - Obstacles to adoption, and a way forward. Proceedings - 9th International Conference on Availability, Reliability and Security, ARES 2014, 158–165. https://doi.org/10.1109/ARES.2014.28

Cegielski, C. G., Allison Jones-Farmer, L., wu, Y., & Hazen, B. T. (2012). Adoption of cloud computing technologies in supply chains: An organizational information processing theory approach. The International Journal of Logistics Management, 23(2), 184–211. https://doi.org/10.1108/09574091211265350

Chan, W., Leung, E., & Pili, H. (2012). COSO Enterprise Risk Management for Cloud Computing.

Chang, C. C., Li, C. T., & Shi, Y. Q. (2018). Privacy-Aware Reversible Watermarking in Cloud Computing Environments. IEEE Access, 6, 70720–70733. https://doi.org/10.1109/ACCESS.2018.2880904

Coss, D. L., & Dhillon, G. (2019). Cloud privacy objectives a value based approach. Information and Computer Security, 27(2), 189–220. https://doi.org/10.1108/ICS-05-2017-0034

Delavari, V., Shaban, E., Janssen, M., & Hassanzadeh, A. (2020). Thematic mapping of cloud computing based on a systematic review: a tertiary study. Journal of Enterprise Information Management, 33(1), 161–190. https://doi.org/10.1108/JEIM-02-2019-0034

Doherty, E., Carcary, M., & Conway, G. (2015). Migrating to the cloud examining the drivers and barriers to adoption of cloud computing by smes in ireland: An exploratory study. Journal of Small Business and Enterprise Development, 22(3), 512–527. https://doi.org/10.1108/JSBED-05-2013-0069

Dwivedi, Y. K., & Mustafee, N. (2010). It's unwritten in the Cloud: The technology enablers for realising the promise of Cloud Computing. Journal of Enterprise Information Management, 23(6), 673–679. https://doi.org/10.1108/17410391011088583

El-Gazzar, R. F. (2014). An overview of cloud computing adoption challenges in the norwegian context. Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014, 412–418. https://doi.org/10.1109/UCC.2014.52

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. Journal of Systems and Software, 118, 64–84. https://doi.org/10.1016/j.jss.2016.04.061

Eze, B., Kuziemsky, C., & Peyton, L. (2018). Operationalizing privacy compliance for cloud-hosted sharing of healthcare data: A case study. Proceedings - International Conference on Software Engineering, 18–25. https://doi.org/10.1145/3194696.3194701

Fatima, A., & Colomo-Palacios, R. (2018). Security aspects in healthcare information systems: A systematic mapping. Procedia Computer Science, 138, 12–19. https://doi.org/10.1016/j.procs.2018.10.003

Feng, B., Lin, Y., Xu, T., & Duan, J. (2021). A survey on privacy preservation in video big data. International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2021, 55(1). https://doi.org/10.1109/ICECCME52200.2021.9591105

Ferri, L., Spanò, R., Maffei, M., & Fiondella, C. (2020). How risk perception influences CEOs' technological decisions: extending the technology acceptance model to small and medium-sized enterprises' technology decision makers. European Journal of Innovation Management, 24(3), 777–798. https://doi.org/10.1108/EJIM-09-2019-0253

Fu, C., Lv, Q., & Badrnejad, R. G. (2020). Fog computing in health management processing systems. Kybernetes, 49(12), 2893–2917. https://doi.org/10.1108/K-09-2019-0621

Gao, F., & Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. International Journal of Information Management, 48(July 2018), 120–138. https://doi.org/10.1016/j.ijinfomgt.2019.02.002

Ghahramani, M. H., Zhou, M., & Hon, C. T. (2017). Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services. IEEE/CAA Journal of Automatica Sinica, 4(1), 6–18. https://doi.org/10.1109/JAS.2017.7510313

Grob, M., Cheng, V., Burns, J. (2021). COSO Enterprise Risk Management for Cloud Computing, COSO, https://www.coso.org/Documents/COSO-ERM-for-Cloud-Computing.pdf

Grubisic, I. (2014). ERP in clouds or still below. Journal of Systems and Information Technology, 16(1), 62–76. https://doi.org/10.1108/JSIT-05-2013-0016

Hampton, J. (2009). Fundamentals of Enterprise Risk Management.

Han, S., Han, K., & Zhang, S. (2019). A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era. IEEE Access, 7, 60290–60298. https://doi.org/10.1109/ACCESS.2019.2914862

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153(January), 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Hopkin, P. (2017). Fundamentals of Enterprise Risk Management – Understanding, evaluating and implementing effective risk management.

Iqbal, A., & Colomo-Palacios, R. (2019). Key Opportunities and Challenges of Data Migration in Cloud: Results from a Multivocal Literature Review. Procedia Computer Science, 164, 48–55. https://doi.org/10.1016/j.procs.2019.12.153

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers, 24(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

ISO31000. (2018). BS ISO 31000: 2018 BSI Standards Publication Risk management — Guidelines. BSI Standards Publication, 26.

Kajiyama, T., Jennex, M., & Addo, T. (2017). To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. Information and Computer Security, 25(5), 634–659. https://doi.org/10.1108/ICS-07-2016-0051

Kauffman, R. J., Ma, D., & Yu, M. (2018). A metrics suite of cloud computing adoption readiness. Electronic Markets, 28(1), 11–37. https://doi.org/10.1007/s12525-015-0213-y

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kitchenham, B.A, Budgen, D., Brereton, P., (2016). Evidence-Based Software Engineering and Systematic Reviews. CRC Press

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4–5), 372–386. https://doi.org/10.1016/j.telpol.2012.04.011

Kuo, M. (2011) Opportunities and Challenges of Cloud Computing to Improve Health Care Services, J Med Internet Res 2011;13(3):e67, https://www.jmir.org/2011/3/e67

Kuzminykh, L., Ghita, B., Sokolov, V., Bakhshi, T. (2021). Information Security Risk Assessment. Encyclopedia 2021, 1, 602 – 617. https://doi.org/10.3390/encyclopedia1030050

Landoll, D, (2021). The Security Risk Assessment Handbook

Li, H., Liu, L., Lan, C., Wang, C., & Guo, H. (2020). Lattice-Based Privacy-Preserving and Forward-Secure Cloud Storage Public Auditing Scheme. IEEE Access, 8, 86797–86809. https://doi.org/10.1109/ACCESS.2020.2991579

Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. International Journal of Information Management, 34(1), 28–36. https://doi.org/10.1016/j.ijinfomgt.2013.09.004

Lu, Z., Qian, P., Bi, D., Ye, Z., He, X., Zhao, Y., Su, L., Li, S., & Zhu, Z. (2021). Application of AI and IoT in Clinical Medicine: Summary and Challenges. 41(6), 1134–1150.

Maeser, R. (2020). Analyzing CSP Trustworthiness and Predicting Cloud Service Performance. IEEE Computer Graphics and Applications, May, 73–85. https://doi.org/10.1109/OJCS.2020.2994095

Maniah, Soewito, B., Lumban Gaol, F., & Abdurachman, E. (2021). A systematic literature Review: Risk analysis in cloud migration. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.01.008

Masuda, Y., Shirasaka, S., Yamamoto, S., & Hardjono, T. (2017). Risk Management for Digital Transformation in Architecture Board: A Case Study on Global Enterprise. Proceedings - 2017 6th IIAI International Congress on Advanced Applied Informatics, IIAI-AAI 2017, 255–262. https://doi.org/10.1109/IIAI-AAI.2017.79

Mbunge, E., Muchemwa, B., Jiyane, S., & Batani, J. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. Global Health Journal, 5(4), 169–177. https://doi.org/10.1016/j.glohj.2021.11.008

Mekawie, N., & Yehia, K. (2021). Challenges of deploying cloud computing in eHealth. Procedia Computer Science, 181(2019), 1049–1057. https://doi.org/10.1016/j.procs.2021.01.300

Mitropoulos, S., & Veletsos, A. (2020). A Categorization of Cloud-Based Services and their Security Analysis in the Healthcare Sector. SEEDA-CECNSM 2020 - 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference. https://doi.org/10.1109/SEEDA-CECNSM49515.2020.9221808

Mohammad, O. K. J. (2018). Recent trends of cloud computing applications and services in medical, educational, financial, library and agricultural disciplines. ACM International Conference Proceeding Series, 132–141. https://doi.org/10.1145/3233347.3233388

Mourtzis, D., & Vlachou, E. (2016). Cloud-based cyber-physical systems and quality of services. TQM Journal, 28(5), 704–733. https://doi.org/10.1108/TQM-10-2015-0133

NHS Digital. Health and Social Care Cloud Risk Framework. NHS Digital; 2018.

Onwuegbuzie, A.J., Leech, N.L., Collins, K.M.T., (2012), Qualitative Analysis Techniques for the Review of the Literature. The Qualitative Report, 17, 56, 1-28. http://www.nova.edu/ssss/QR/QR17/onwuegbuzie.pdf

Piliouras, T., Yu, P. L. R., Su, Y., Siddaramaiah, V. K. A., Sultana, N., Meyer, E., & Harrington, R. (2011). Trust in a cloud-based healthcare environment. 2011 8th International Conference and Expo on Emerging Technologies for a Smarter World, CEWIT 2011. https://doi.org/10.1109/CEWIT.2011.6135890

Poorejbari, S., & Vahdat-Nejad, H. (2015). An Introduction to Cloud-Based Pervasive Healthcare Systems. PerCAM14 2014 https://doi.org/10.4108/icst.iccasa.2014.257442

Rahman, R., & Mahmud, T. (2021). Integrating Cloud Computing in E-healthcare: System Design, Implementation and Significance in Context of Developing Countries.

Ranaweera, P., Jurcut, A., & Liyanage, M. (2022). MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. ACM Computing Surveys, 54(9), 1–37. https://doi.org/10.1145/3474552

Rehman, U. U., Park, S. B., & Lee, S. (2021). Secure Health Fog: A Novel Framework for Personalized Recommendations Based on Adaptive Model Tuning. IEEE Access, 9, 108373–108391. https://doi.org/10.1109/ACCESS.2021.3101308

Savvides, S., Kumar, S., Stephen, J. J., & Eugster, P. (2021). C3PO: Cloud-based Confidentiality-preserving Continuous. ACM Transactions on Privacy and Security. 25(1).

Shanmugapriya, E., & Kavitha, R. (2019). Efficient and Secure Privacy Analysis for Medical Big Data Using TDES and MKSVM with Access Control in Cloud. Journal of Medical Systems, 43(8). https://doi.org/10.1007/s10916-019-1374-6

Sharma, M., & Sehrawat, R. (2020). Quantifying SWOT analysis for cloud adoption using FAHP-DEMATEL approach: evidence from the manufacturing sector. Journal of Enterprise Information Management, 33(5), 1111–1152. https://doi.org/10.1108/JEIM-09-2019-0276

Singh, P., Dwivedi, Y. K., Kahlon, K. S., Sawhney, R. S., Alalwan, A. A., & Rana, N. P. (2020). Smart Monitoring and Controlling of Government Policies Using Social Media and Cloud Computing. Information Systems Frontiers, 22(2), 315–337. https://doi.org/10.1007/s10796-019-09916-y

Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications, 178(July 2020), 102950. https://doi.org/10.1016/j.jnca.2020.102950

Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., Halunga, S., & Fratu, O. (2015). Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications. Journal of Medical Systems, 39(11). https://doi.org/10.1007/s10916-015-0327-y

Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management, 34(2), 177–184. https://doi.org/10.1016/j.ijinfomgt.2013.12.011

Sun, P. J. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160(August 2019), 102642. https://doi.org/10.1016/j.jnca.2020.102642

Tebaa, M., & Hajji, S. el. (2014). From Single to Multi-clouds Computing Privacy and Fault Tolerance. IERI Procedia, 10, 112–118. https://doi.org/10.1016/j.ieri.2014.09.099

Wakunuma, K., & Masika, R. (2017). Cloud computing, capabilities and intercultural ethics: Implications for Africa. Telecommunications Policy, 41(7–8), 695–707. https://doi.org/10.1016/j.telpol.2017.07.006

Wu, Y., Lyu, Y., & Shi, Y. (2019). Cloud storage security assessment through equilibrium analysis. Tsinghua Science and Technology, 24(6), 738–749. https://doi.org/10.26599/TST.2018.9010127

Xu, J., Liang, C., Jain, H. K., & Gu, D. (2019). Openness and security in cloud computing services: Assessment methods and investment strategies analysis. IEEE Access, 7, 29038–29050. https://doi.org/10.1109/ACCESS.2019.2900889

Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2022). Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. ACM Computing Surveys, 54(8). https://doi.org/10.1145/3456628

Appendix

Paper ID	Title	Author
S1	“Trust in a cloud-based healthcare environment”	“Piliouras, T. Yu, P.LR. Su, Y. Siddaramaiah, V. Kumar A. Sultana, N. Meyer, E. Harrington, R.”
S2	“Healthcare services in the cloud - obstacles to adoption, and a way forward”	“Bernsmed, K. Cruzes, D. S. Jaatun, M. G. Haugset, B.G., Erlend A.”
S3	“Risk management for digital transformation in architecture board: a case study on global enterprise”	“Masuda, Y. Shirasaka, S. Yamamoto, S. Hardjono, T.”
S4	“Risk analysis of cloud sourcing in healthcare and public health industry”	“Abrar, H.H., Syed, J. Chaudhry, Junaid Saleem, K. Orgun, M.A. Al-Muhtadi, J. Valli, C.”
S5	“Internet of things security: a review of risks and threats to healthcare sector”	“Abouzakhar, N. S., Jones, A. Angelopoulou, O.”
S6	“A categorization of cloud-based services and their security analysis in the healthcare sector”	“Mitropoulos, S., Veletsos, A.”
S7	"Integrating cloud computing in e-healthcare: system design, implementation, and significance in the context of developing countries"	“Rahman, R. Mahmud, T.”
S8	“Secure health fog: a novel framework for personalized recommendations based on adaptive model tuning”	“Rehman, U.U. Park, S.B. Lee, S.”
S9	“Trust model for efficient honest broker-based healthcare data access and processing”	“Alarcon, M.L Nguyen, M. Debroy, S. Bhamidipati, N.R. Calyam, P. Mosa, A.”
S10	“An overview of cloud computing adoption challenges in the Norwegian context”	“El-Gazzar, R.F.”
S11	“An introduction to cloud-based pervasive healthcare systems”	“Poorejbari, S, Vahdat-Nejad, H.”
S12	"Cloud computing adoption readiness assessment in Saudi healthcare organizations: a strategic view"	“Alharbi, F. Atkins, A. Stanier, C.”
S13	“Operationalizing privacy compliance for cloud-hosted sharing of healthcare data: a case study”	“Eze, B. Kuziemsky, C. Peyton, L.”
S14	“Recent trends of cloud computing applications and services in medical, educational, financial, library and agricultural disciplines”	“Mohammad, O.K.J.”
S15	“A survey on privacy preservation in fog-enabled internet of things”	“Feng, B. Lin, Y. Xu, T. Duan, J.”
S16	“C3po: cloud-based confidentiality-preserving continuous query processing”	“Savvides, S. Kumar, S. Stephen, J.J. Eugster, P.”
S17	“Integrated blockchain and cloud computing systems: a systematic survey, solutions, and challenges”	“Zou, J. He, D. Zeadally, S. Kumar, N. Wang, H. Choo, K.R.”
S18	“MEC-enabled 5g use cases: a survey on security vulnerabilities and countermeasures”	“Ranaweera, P. Jurcut, A. Liyanage, M.”
S19	“Privacy and security issues in cloud computing: the role of institutions and institutional evolution”	“Kshetri, N.”
S20	“Making use of cloud computing for healthcare provision: opportunities and challenges”	“Sultan, N.”
S21	“From single to multi-clouds computing privacy and fault tolerance”	“Tebaa, M. Hajji, E.S”
S22	“An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital”	“Lian, J.W Yen, D.C. Wang, Y.T.”
S23	“Understanding cloud computing adoption issues: a Delphi study approach”	“El-Gazzar, R Hustad, E Olsen, D.H.”
S24	“Cloud computing, capabilities and intercultural ethics: implications for Africa”	“Wakunuma, K Masika, R”

Paper ID	Title	Author
S25	“Cloud computing-enabled healthcare opportunities, issues, and applications: a systematic review”	“Ali, O. Shrestha, A. Soar, J. Wamba, S.F.”
S26	“Key issues for embracing the cloud computing to adopt a digital transformation: a study of Saudi public sector”	“Al-Ruithe, M. Benkhelifa, E. Hameed, K.”
S27	“Security aspects in healthcare information systems: a systematic mapping”	“Fatima, A. Colomo-Palacios, R.”
S28	"Key opportunities and challenges of data migration in the cloud: results from a multivocal literature review"	“Iqbal, A. Colomo-Palacios, R.”
S29	“An exhaustive survey on security and privacy issues in healthcare 4.0”	“Hathaliya, J.J. Tanwar, S.”
S30	“Security and privacy of electronic health records: concerns and challenges”	“Keshta, I. Odeh, A.”
S31	“Security and privacy protection in cloud computing: discussions and challenges”	“Sun, P.”
S32	“Validation of architectural requirements for tackling cloud computing barriers: cloud provider perspective”	“Alghamdi, B. Potter, L.E. Drew, S.”
S33	“Challenges of deploying cloud computing in e-health”	“Mekawie, N. Yehia, K.”
S34	“A systematic literature review: risk analysis in cloud migration”	“Maniah, Soewito, B., Gaol, F.L., Abdurachman, E.”
S35	“Advances on networked e-health information access and sharing: status, challenges and prospects”	“Aski, V.J. Dhaka, V.S. Kumar, S. Verma, S. Rawat, D.B.”
S36	“Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies”	“Mbunge, E. Muchemwa, B. Jiyane, S. Batani, J.”
S37	“Blockchain technology as a fog computing security and privacy solution: an overview”	“Alzoubi, Y.I. Al-Ahmad, A. Kahtan, H.”
S38	“A metrics suite of cloud computing adoption readiness”	“Kauffman, R.J. Ma, D. Yu, M.”
S39	“Big data, internet of things and cloud convergence – an architecture for secure e-health applications”	“Suciu, G. Suciu, V. Martian, A. Craciunescu, R. Vulpe, A. Marcu, I. Halunga, S. Fratu, O.”
S40	“Efficient and secure privacy analysis for medical big data using TDES and MKSVM with access control in cloud”	“Shanmugapriya, E. Kavitha, R.”
S41	“Transforming business using digital innovations: the application of ai, blockchain, cloud and data analytics”	“Akter, S. Michael, K. Uddin, M.R McCarthy, G. Rahman, M.”
S42	“Application of ai and IoT in clinical medicine: summary and challenges”	“Lu, Z. Qian, P. Bi, D. Ye, Z. He, X. Zhao, Y. Su, L. Li, S. Zhu, Z.”
S43	“Let me in the cloud: analysis of the benefit and risk assessment of cloud platform”	“Aleem, A., Ryan, S.C.”
S44	“Adoption of cloud computing technologies in supply chains: an organizational information processing theory approach”	“Cegielski, C.G. Allison Jones-Farmer, L. Wu, Y. Hazen, B.T.”
S45	“ERP in clouds or still below”	“Grubisic, I.”
S46	“Migrating to the cloud examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: an exploratory study”	“Doherty, E. Carcary, M. Conway, G.”
S47	“Cloud-based cyber-physical systems and quality of services”	“Mourtzis, D. Vlachou, E.”
S48	“To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions”	“Kajiyama, T. Jennex, M. Addo, T.”
S49	“Cloud privacy objectives a value-based approach”	“Coss, D.L. Dhillon, G.”
S50	“How risk perception influences CEOs’ technological decisions: extending the technology acceptance model to small and medium-sized enterprises' technology decision makers”	“Ferri, L., Spanò, R., Maffei, M., Fiondella, C.”
S51	“Towards a maturity model for health-care cloud security (m2hcs)”	“Akinsanya, O., Papadaki, M., Sun, L.”
S52	“Thematic mapping of cloud computing based on a systematic review: a tertiary study”	“Delavari V,.Shaban E., Janssen M., Hassanzadeh A.”

Paper ID	Title	Author
S53	"Quantifying swot analysis for cloud adoption using fahp-dematel approach: evidence from the manufacturing sector"	"Sharma M., Sehrawat R."
S54	"Fog computing in health management processing systems"	"Fu C., Lv Q., Badrnejad R."
S55	"E-health cloud: opportunities and challenges "	"AbuKhousa, E. Mohamed, N. Al-Jaroodi, J."
S56	"Toward cloud computing QOS architecture: analysis of cloud systems "and cloud services"	"Ghahramani, M. H. Zhou, M. Hon, C.T."
S57	"Privacy-aware reversible watermarking in cloud computing environments"	"Chang, C.C. Li, C.T. Shi, Y.Q."
S58	"Openness and security in cloud computing services: assessment methods and investment strategies analysis"	"Xu, J. Liang, C. Jain, H.K. Gu, D."
S59	"A data sharing protocol to minimize security and privacy risks of cloud storage in big data era"	"Han, S. Han, K. Zhang, S."
S60	"Cloud computing: overview and risk identification based on classification by type"	"Belbergui, C. Elkamoun, N. Hilal, R."
S61	"Cloud storage security assessment through equilibrium analysis"	"Wu, Y. Lyu, Y. Shi, Y."
S62	"Analyzing CSP trustworthiness and predicting cloud service performance"	"Maeser, R."
S63	"Lattice-based privacy-preserving and forward-secure cloud storage public auditing scheme"	"Li, H. Liu, L. Lan, C. Wang, C. Guo, H."