Chapter 1

Cloud Computing Economic Risks and Challenges

Serkan Özdemir[1]

Abstract

In today's highly competitive business environment, cloud computing offers significant advantages for many companies, but it also presents substantial risks and challenges. Both operational and financial risks can deter businesses from adopting cloud-based systems, and in some cases, these risks may even threaten the survival of the firm. The financial concerns include unexpected costs, reliance on third-party providers, and difficulties in predicting long-term expenses, which can make cloud adoption a risky venture for some organizations. This research aims to systematically identify the financial risks and challenges associated with cloud computing through a Systematic Literature Review (SLR). By analyzing existing studies, the study will uncover the most common financial difficulties faced by firms and propose several solutions to address these issues. To validate the proposed remedies, a cost-benefit analysis will be conducted, ensuring that the solutions are practical and financially viable for businesses considering cloud adoption. This study seeks to provide firms with a clearer understanding of the financial risks involved in cloud computing and offer strategies to mitigate these challenges, making cloud integration a more secure and manageable option for businesses in a competitive market.

1. Introduction

The pandemic's recent global efforts have drawn attention to the dangers and difficulties associated with IT-related procedures. Particularly, the new home-office working model reveals fresh risks that could put the business in danger of financial collapse. The reason for this is that businesses are turning to cloud computing solutions rather than internal data storage techniques.

1 Arş. Gör. Dr., Orta Doğu Teknik Üniversitesi, serkano@metu.edu.tr, ORCID ID: 0000-0002-8635-3311

https://doi.org/10.58830/ozgur.pub574.c2352

As a result, it's critical to evaluate the risks and difficulties that could cause a company to experience a financial slump and identify countermeasures.

Cloud computing is widely used in information technology. However, since pertinent security technologies are still in their infancy, many service providers are still hesitant to completely implement the system related unpredictable risks. Additionally, cloud security risks are rising significantly as new technologies are developed to satisfy user requests. These risks take the shape of multiple hidden exploits using cloud computing services and the interfaces that go along with them. Because cloud computing offers high-quality, low-cost internet services with a high economic value, it impacts many industries, including e-commerce. Without a doubt, this is the next big thing in business and the internet.

By delving deeper into the financial effects on businesses, this study expands on previous research that concentrated on the two most important components of cloud systems: risk assessment [1] and security challenges [2]. In order to obtain quantitative insights into the viability of suggested remedies for the issues, it also does cost-benefit analysis. The literature review, system model description, problem approach, analytical and experimental results, potential work expansions, discussion, and conclusion make up the paper's components. Based on a literature study, it is examined and evaluated the most significant risks to cloud systems regarding network and data security.

2. Literature Review

The following study topics were determined in order to perform a Systematic Literature Review on economic risks and challenges of cloud computing in e commerce:

RQ1: What are the threats to the long-term financial viability of cloud computing companies?

RQ2: What are the threats to the long-term viability of the economy that cloud computing users face?

In light of the research scope, the research questions are identified, and specific keywords are chosen. The terms "cloud AND comput* AND econom*" and "cloud AND comput* AND econom* AND risk*" refer to the research questions and review protocol, respectively. A title, abstract, or keyword occurrence is looked for. The databases Web of Science and Scopus are utilized for Systematic Literature Review (SLR). Specific inclusion and exclusion criteria are utilized to focus the investigation. Articles, conference

proceedings, and book chapters were identified as the threshold qualities for papers. During the SLR process, only published articles with open access were taken into account. A Quality Assessment Checklist (QAC) was created so that each and every study could be evaluated. The following criteria define the questions on the checklist: a) Is the study technique clearly mentioned in the research paper? b) Is the approach appropriate for the particular problem?

Figure 1 outlines the entire process of selection. The criteria were established in accordance with the quality assessment checklist and the study's applicability to the goal of the investigation.

68 studies in all were discovered throughout the database search. After these articles were subjected to QAC and inclusion/exclusion criteria, 32 publications were identified as primary studies for analysis. Studies pertaining to obstacles were added during the inclusion process. Studies with a scope that was irrelevant, as well as dangers and obstacles pertaining to areas other than the economic impact, were removed.

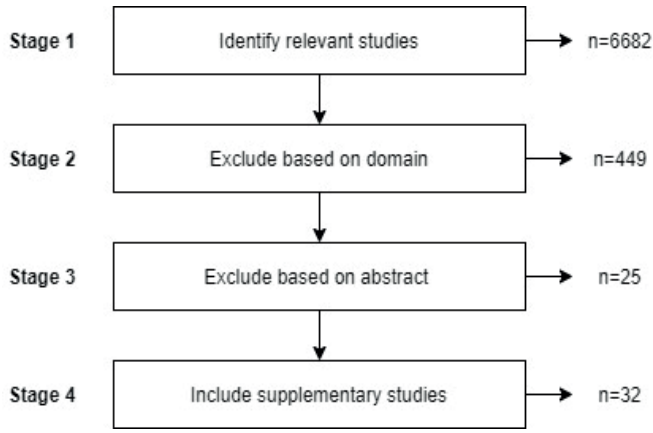

Figure 1. Study selection process

The articles reviewed and included in this research are shown in Figure 2. The data is distributed in terms of publication years. The relationship between cloud security and organizational level has not been extensively studied. Because of this, current revive on cloud-based service models has tended to focus on operational and technological concerns rather than security concerns specific to cloud computing. Though these have been few in number, some studies have looked at cloud service adoption from an organizational perspective in relation to security breaches. In keeping with

the objectives of the study, this revive discusses the weaknesses in cloud security in an organizational setting.

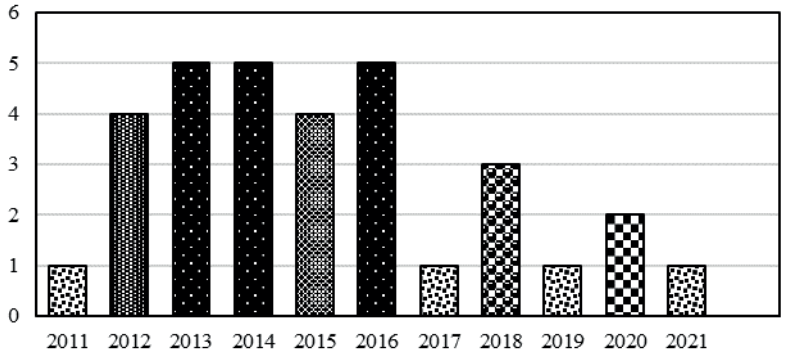

Figure 2. Paper distribution per years

Based on the degree to which the interconnected dangers that cloud computing providers and clients face were assessed, the selected papers were subjected to in-depth study. Then, thirteen main categories of cloud computing-related risks were defined, taking into account the perspectives of both cloud providers and customers as well as research questions and publications. The categories that have been identified are resource utilization, data leakage, pricing strategy, trust, unforeseen circumstances, security, consumer adoption of cloud computing, information asymmetry, vendor lock-in, integration, backup strategy, investment strategy, and overload. Table 1 summarizes the risks associated with providers.

Table 1. Summary of the Provider Risks

Cloud Provider Risks	**List of Studies**
Resource Utilization	[3], [4], [5], [6]
Data Leakage	[7]
Pricing Strategy	[8], [9]
Trust	[10]
Unforeseen Circumstances	[11]
Security	[9], [12]
Customer Cloud Adoption	[13]

Summary of customer risks can be seen in Table 2. The research studies are concentrated on mainly data leakage, vendor lock-in and security to

protect the customer against the various risk and ensuring the security of cloud computing. Studies on integration, asymmetry of information, back-up strategy and overload are rather scarce.

Table 2. Summary of the Customer Risks

Cloud Customer Risks	**List of Studies**
Data Leakage	[14], [15], [16], [17], [18], [12], [19], [20]
Asymmetry of Information	[21]
Vendor Lock-in	[22], [23], [24], [25], [26], [20]
Integration	[27]
Back-Up Strategy	[28]
Investment Strategy	[29], [26], [30]
Overload	[31]
Security	[19], [20], [25], [26], [32], [33]

2.1. RQ1: Risks from Cloud Providers Perspective

From the standpoint of the suppliers, resource utilization is the most significant risk. According to Dartois et al. [3], excessive commitment to recovering underutilized resources may result in diminished cloud provider integrity and overrun capacity, which could have a negative financial impact. Furthermore, Shahrad and Wentzlaff noted that there is a chance that service users won't receive the availability guarantee, which could result in lost income [4]. Furthermore, because suppliers may not be able to meet future demand, capacity planning poses a significant financial risk, according to Qanbari et al. [5]. Finally, Vázquez et al. note that when providers wish to enhance capacity use, there is a danger of infrastructure resource exhaustion, which ultimately results in price penalties and customer churn [6].

Pricing strategy is a significant economic risk as well. According to Jain et al., implementing a very unrealistic pricing plan for cloud services could result in small firms going bankrupt and cloud providers losing their revenue stream [8]. In addition, August et al. assert that a well-thought-out pricing strategy is necessary to encourage riskier consumption [9].

In the long-term, security undermines supplier credibility as well. According to August et al., inadequate user patching behavior increases the chance of malicious program infection, which can quickly spread throughout weak software networks and result in significant financial harm. Because of their enormous service populations, cloud services, especially the Software as

a Service (SaaS) variants, are more vulnerable. Furthermore, there's a chance that security breaches will cause financial harm [9]. In addition, according to Aminnezhad et al., there is a chance that cloud services providers' reputation and trustworthiness could be damaged by a cyberattack. Service level agreements need to be strong enough to withstand any danger from cybercrime [12].

Multitenancy may result in data leakage when clients were untrusted users, which might ultimately harm brand equity, according to Almutairi et al. [7]. However, Nowicka noted that a risk associated with trust keeps cloud computing from reaching its true potential [10]. Chang has also contributed to the research by stating that the economic structure paradigm of cloud providers may be impacted by the possibility of a financial crisis, natural calamities, or accidents [11]. Chang concluded by saying that consumers' strategies for adopting cloud computing carry a commensurate degree of risk, particularly when it comes to bad adoption decisions, excessive spending, and incorrect equipment selections [13].

2.2. RQ2: Risks from Cloud Customers Perspective

From the standpoint of the clients, data leaking is the biggest concern. According to Zhang and Gong, cloud customers who utilize supply chain management systems run some dangers when they share information with suppliers. Authors claim that disclosing information could cause financial harm in any dispute [14]. Furthermore, Kodym et al. noted that openness and data sharing could make businesses more susceptible to physical and cyber threats, raising operating expenses. It also has negative effects on negotiations with other parties [15]. Furthermore, Wei et al. noted that relying on a trusted third party carries a risk of data leakage, which could include important information shared during cloud data sharing services [16]. In the meantime, Kamhoua et al. claimed that when a business discloses its vulnerabilities, there is a significant chance that the information will be leaked to the public and attackers, decreasing the company's market share, income, and reputation [17]. Further input from Koo and Kim indicated that if the necessary expenditure is not managed correctly during cloud computing adoption, there is a danger of significant losses to the organization due to data leakage [18]. Furthermore, Aminnezhad et al. claim that when businesses use public clouds, buying computing services from outside sources may put their data security at risk. Leaning toward private cloud could be one way to avoid this. However, because it requires additional infrastructure, this solution comes at an exponentially higher cost [12]. Furthermore, Islam et al. note that cloud computing presents

some security, privacy, and data management concerns for businesses integrating it into their systems. Any intrusion could result in the disclosure of private data, a breakdown in services, and enormous financial damages [19]. Furthermore, Rostek et al. note that cloud computing carries various dangers, like vendor lock-in, security/cyberattack threats, and data leakage, which could be costly for businesses [20].

Vendor lock-in is a significant additional challenge. According to Kitchin and Dodge, there is a long-term risk of financial strain and overdependence when using cloud services because of their intrinsic trustworthiness [22]. On the other hand, Horvath et al. claim that the main implementation risk for businesses would be vendor lock-in [23]. Furthermore, Ghachem et al. note that a major problem arises when there is a decentralized distributed computation capability that undermines the provider's credibility. In addition, in the event that a corporation grows, vendor dependence raises the risk of operational expense management [24]. Additionally, Brender and Markov highlight a number of hazards that clients employing cloud computing in their business face and which may have an indirect impact on their financial status. These risks include vendor lock-in, information security, user access privileges, regulatory compliance, and disaster recovery [25]. Furthermore, according to Rabaey, a well-defined implementation plan is necessary to avoid service provider lock-in. Prior to use cloud computing services, it is advisable to take macroeconomic factors and material costs into account [26]. Moreover, Rostek et al. note that cloud computing carries some dangers, like vendor lock-in, security/cyberattack threats, and data leakage, which could be costly for businesses [20].

Another aspect of hazards associated to customers is security. Using cloud computing in their business comes with a number of dangers, according to Brender and Markov [25]. These risks include information security, user access privileges, regulatory compliance, disaster recovery, and vendor lock-in. Additionally, Kronabeter and Fenz note that cloud computing users run the danger of having their data location, regulatory compliance, and user access credentials compromised, which could have an indirect negative impact on their financial structure [32]. In addition, Islam et al. note that cloud computing presents certain security, privacy, and data management concerns for businesses integrating it into their systems. Any intrusion could result in the disclosure of private data, a breakdown in services, and enormous financial damages [19]. Furthermore, Rabaey states that moving personnel to different departments during the SaaS deployment period poses a risk and could perhaps invite strikes. This ultimately has an impact on the organizational level and how business is conducted [26]. Moreover,

Thomas notes that security-related concerns rank among the major obstacles that cloud computing may provide to the operation of businesses [33]. Additionally, cloud computing has hazards according to Rostek et al. that could cost businesses money, like vendor lock-in, security/cyberattack threats, and data loss [20].

Investment strategy affects the financial position of cloud computing deployments. According to Khan et al., there is a chance that a decision support system won't be able to meet user needs, which could lead to the incorrect investment choice [29]. Furthermore, Rabaey states that moving personnel to different departments during the SaaS deployment period poses a risk and could perhaps invite strikes. This ultimately has an impact on the organizational level and how business is conducted [26]. In addition, Chou and Oetting note that while cloud computing helps businesses save money on initial investments by avoiding the need to buy infrastructure, the financial advantages of cloud computing will diminish if resource provisioning is overestimated or underestimated [30].

Ayaburi, Maasberg, and Lee assert that customers may select less profitable and riskier cloud providers as a result of information asymmetry with cloud providers. Additionally, when a vendor presents contractual issues in a table, it could put a heavy weight on the customers [21]. Remondino, however, asserted that cloud computing technologies pose a risk to content ownership, business continuity, and other regulatory requirements. Additionally, it might integrate with current internal systems [27]. Wang et al. have added to the body of knowledge by stating that failure is possible if the backup plan is not dependable and economical. Furthermore, various services with varying turnaround times and processing capacities necessitate a thorough backup plan that takes dependability and cost into account [28]. Last but not least, Marbukh noted that there is a trade-off in cloud computing between the systemic risk of cascading overload and economic loss [31].

2.3. Research Problem

The outcomes of SLR assist in identifying areas of cloud computing economics study that warrant further investigation. Data leakage-related problems that impact both the provider and the customer would be one captivating topic. Issues from the provider side arise when multitenancy cloud computing is used, and as trust is a key factor in cloud service selection, there is a possibility that this could cause significant harm to brand equity and financial loss. Insider leaks and supplier leaks are related to customer-side issues. Any kind of data leak might land the company in serious legal

hot water, resulting in fines and difficulties when negotiating with other parties.

3. Description of the Systems Model

The research issue of the financial effects of data leaking on businesses has a number of remedies. Four of the most practical fixes for the data leaking issue are suggested.

3.1. Solution 1: Access Control Mechanism

Generally, not every employee in a company needs the same level of access to sensitive data. Employees who rarely need access to information should be given authorization to prevent information from falling into the wrong hands. Additionally, it is preferable to set a document's sharing settings to "view" rather than "edit." As long as the company maintains track of personnel changes, granting access through the IT department is easy to administer. Furthermore, the corporation needs to guarantee that any departing personnel are immediately denied access.

Additionally, the owner of the data should authorize a specific group so that handling data access is simple. Security standards that are created from data-related information can be used to protect data and prevent problems from arising in particular departments, thereby guaranteeing access control of the data.

Technologies known as access control methods limit access to users who are permitted and forbid access from unauthorized sources [34]. Therefore, it is necessary to provide clear means to manage access permissions to the system and services. These kinds of processes ought to cover the complete user access lifecycle, from initial user registration through the deactivation of user access that isn't necessary for using the system or its services. When appropriate, the need to govern the distribution of access privileges—which enable users to get around system controls—should receive the necessary attention. To create a workable control management system for user access, these six control assertions are crucial:

1. Maintain a record of who can access what data.
2. Manage the permissions for user access.
3. Encourage appropriate access protocols.
4. Control user access to network services.
5. Monitor who is able to access which operating systems.

6. Control system and application access.

Under the SaaS model, the cloud provider typically oversees every aspect of the network, including the servers and other equipment. In this paradigm, network-based limitations are superfluous because the program is provided as a service to its clients, who are typically in charge of it through a web browser. Instead, user access techniques like one-time password control take their place. In order to enhance the security of data stored via SaaS, users must prioritize user access procedures like provisioning and authentication.

In the Platform as a Service (PaaS) cloud model, access control to the entire network and associated infrastructure is under the control of the cloud provider. However, the client bears the majority of the burden for access control to programs hosted on a PaaS platform. User provisioning and authentication are included in user access management, one of the many varieties of user access management systems. Infrastructure as a Service (IaaS) users are entirely in charge of all aspects of access control to their cloud resources. The client is responsible for designing and overseeing the storage, network, and hosted applications on IaaS, as well as virtual server access. Within the IaaS cloud paradigm, access management can be classified into two categories. The user is in charge of access control to its virtual server, networks, storage, and applications stored on virtual servers, while the cloud provider owns and controls access control to the host, network, and management apps.

3.2. Solution 2: Data Encryption

It is advised to employ encryption to protect data when it is being transferred, stored, or used in any other manner. To read data that has been encrypted and kept on the cloud, a distinct encryption key is needed. Sensitive information sent between devices and data saved in the cloud should not be stored there unless it is encrypted [35]. Using a secure internet connection is also crucial, especially if it is wanted to stay away from free Wi-Fi hotspots.

Encrypting data is a smart way to keep it safe from unauthorized users while it is waiting to be uploaded to the cloud. If the data is encrypted in IaaS, then it is suggested for Amazon S3. However, because encryption restricts data finding and indexing, it is generally not advised for cloud-based services.

Data exposure may result from government data confiscations for any reason if users share resources in public clouds with other organizations. Data encryption is the only practical way to get around this and improve security in public clouds while also preventing cloud providers from accessing the

data or decrypting the keys. Any third party requesting access to data—whether from the government or another private entity—must get in touch with the user first. This permits data access to the cloud while maintaining user data protection in a more private setting. Even if data is obtained by malevolent people, an encryption technique that renders the data completely unreadable can guarantee a more intricate procedure.

It's critical to assemble, collaborate with several providers, and activate Virtual Security Gateway. This is the best suggested option available to date, and it will help businesses set up their own VPN network with complete encryption connecting all virtual resources around the globe. It will make data transit and communication safer.

The fact that certain suppliers, such as Amazon S3, do not by default offer more secure options is another crucial factor. To avoid unwanted data access, data encryption must be required before starting a backup.

User-level encryption is the most popular method of encrypting data, and it is most frequently employed when the knowledge and resources required for cloud administration have already been amassed.

- Data encryption during transmission; information must be sent from a reliable source with total integrity in addition to being delivered to the right recipient.
- Securing private information before transferring it to a cloud-based platform. It is advised that documents be encrypted with the RSA algorithm and digitally signed.
- Data loss during transmission can be prevented and data integrity guaranteed by cryptographic technologies.

3.3. Solution 3: Use of Central Global Transaction Manager

Global transaction management is the monitoring of transactions that can include actions on two or more different data sources. This feature of transaction processing enables data resources to be returned to their pre-transaction state in the event of an error [35]. Depending on the circumstances, all or none of the resources may be updated.

The 2-phase commit mechanism in Extended Architecture is related to the utilization of a central global transaction manager. Data integrity problems could arise from a combination of SaaS and private apps in the age of service-oriented-architecture and cloud computing. The functionality of SaaS applications is usually provided through XML-based APIs.

3.4. Solution 4: Data Loss Prevention Software

Organizations can employ data loss prevention (DLP) software to ensure compliance and manage important company data. Distribution control, which is required to make sure that users do not share sensitive information across corporate borders, is one of the key components of DLP. Network administrators and security experts establish business rules that specify who has access to view, alter, and share sensitive data. DLP solutions often handle data at both the network and endpoint levels to ensure that policies are consistent throughout the organization. By using these strategies, data security is enabled and data leaks that might be caused by internal actors are prohibited.

While there are some overlaps between DLP technology and some governance, risk, and compliance technologies, the main purpose of these solutions is data control. Additionally, DLP systems can be used in conjunction with backup software, but this is only done as a complement and not in place of it entirely.

For a product to be deemed eligible for the DLP category, it must fulfill the subsequent requirements:

- Monitor data exchange and storage for compliance.
- Admin-level permit control mechanisms as opposed to data governance
- Determine whether there have been any misuses or leaks of data.
- Facilitate the identification and retrieval of data.

4. Approach to the Problem

There are various methods for resolving the issue of data leaking during economic downturns. This study makes four well-known technique recommendations and evaluates each one's viability in light of cost-benefit analysis.

When doing a cost-benefit analysis for an issue, the objective is to determine whether applying the solution will be financially possible and whether the organization will profit while deducting the associated costs. Each category will include a discussion of the costs and advantages associated with various solution options and how they vary in cost-benefit analysis. Direct costs, indirect costs, intangible costs, opportunity costs, and the cost of potential hazards are the primary factors considered when evaluating costs. Conversely, increases in sales and revenue, as well as competitive advantage and intangible benefits, are the primary sources of benefits. 500-person company was taken into consideration when calculating costs and benefits.

4.1. Cost-Benefit Analysis of Solution 1

Cost-benefit analysis of the access control mechanism solution takes into account the costs of hiring staff, providing training, and purchasing network service user access management software, as well as the annual advantages of preserving data loss and building a secure reputation. Table 3 shows that the net profit margin is $5,289,000.

Table 3. Cost-Benefit Analysis of Solution 1

	Dollar Amount ($) (per year)
Costs	
Employee Expense [36]	69,000
Training Expense [37]	50,000
Network service user access management software [38]	12,000
Total Costs	**131,000**
Benefits	
Secure Reputation [39]	1,570,000
Saving data loss expenses that cost on year base [40]	3,900,000
Total Benefits	**5,470,000**
Net Margin	**5,289,000**

4.2. Cost-Benefit Analysis of Solution 2

Employee costs and key storage fees are included in the cost-benefit analysis for data encryption solutions, as is the money saved by lowering the exposure to data breaches. Table 4 shows that the net profit margin is $2,170,000.

Table 4. Cost-Benefit Analysis of Solution 2

	Dollar Amount ($) (per year)
Costs	
Employee Expense (Manager) [41]	108,000
Encryption key storage expense [42]	47,000
Total Costs	**155,000**
Benefits	
Cash saved from reduced data breach exposure [42]	2,325,000
Total Benefits	**2,325,000**
Net Margin	**2,170,000**

4.3. Cost-Benefit Analysis of Solution 3

The central global transaction manager solution's cost-benefit analysis cites mitigating insider attacks and system errors as benefits and employee expenses (four specialists and one manager) as costs. Table 5 shows that the net profit margin is $3,323,000.

Table 5. Cost-Benefit Analysis of Solution 3

	Dollar Amount ($) (per year)
Costs	
Employee Expense (Manager) [41]	108,000
Employee Expense [36]	69,000
Total Costs	**177,000**
Benefits	
Preventing insider attacks and system glitches [43]	3,500,000
Total Benefits	**3,500,000**
Net Margin	**3,323,000**

4.4. Cost-Benefit Analysis of Solution 4

Analyzing the costs and benefits of DLP software solutions come with costs and benefits for the software, staff training, and thwarting insider attacks. Table 6 shows that the net profit margin is $1,742,000.

Table 6. Cost-Benefit Analysis of Solution 4

	Dollar Amount ($) (per year)
Costs	
DLP Software Cost [44]	2,500
Training Expense- IT department(50 employee) [37]	5,000
Total Costs	**7,500**
Benefits	
Preventing insider attacks [43]	1,750,000
Total Benefits	**1,750,000**
Net Margin	**1,742,500**

5. Analytical and Experimental Results

The paper's results were divided into two sections. SLR is the subject of the first section, while the cost-benefit analysis is the subject of the second. The SLR's findings highlighted the dangers and difficulties of adopting cloud computing while taking economic factors into account. From the standpoint of the provider and the client, there are different risks and obstacles. Data leakage from cloud computing and its implications on an organization's financial status are the main topic of this article since, as a result of SLR, this sector has the most references in terms of economic considerations.

The remedies to data leakage and their viability from a cost-benefit perspective are the main topics of the second section of the results. The findings show that every suggested course of action has a net profit margin greater than zero. As a result, each of the remedies may be thought of as a fix for the data leak issue. When compared to other solutions, solution 1 has the highest net profit margin. Thus, in order to avoid any issues with data leaking, enterprises should concentrate on answer 1, which involves implementing access control mechanisms. Conversely, among the other alternatives, solution 4 has the lowest net profit margin, but it also has the lowest cost. For organizations with limited initial funding in such initiatives, it is therefore a more practical choice.

6. Possible Extension to the Work

The data leaking issue was the exclusive focus of this investigation, and solutions were suggested in accordance with the issue. However, as the SLR results show, there are a number of issues, including information asymmetry, vendor lock-in, and integration, that can cause an economic slump for businesses utilizing cloud computing in their systems. Further research is necessary in these areas, taking into account cost-benefit analysis and the financial effects on organizations.

7. Discussion and Conclusion

This study examined the financial risks and difficulties associated with implementing cloud computing from the standpoints of both providers and users. According to the SLR, the number of published articles peaked between 2012 and 2016. Thirty-two articles from the risk and challenge related economic barriers are examined. The outcomes of the thorough evaluation process were compiled at the conclusion. The findings recommend that intriguing facets of the ideas be further developed in the future.

In conclusion, there are various ways to address the issues that cloud computing may bring about in order to avert a financial crisis. The firm must evaluate the solution's advantages and disadvantages and make any necessary modifications before making a final selection, even though cost-benefit analysis is crucial before selecting any other alternatives. However, it is worth noting that the level of security offered by a cloud service is directly related to user acceptance and customization.

References

1. Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: a systematic literature review. *Future information technology*, 285-295.
2. Hussein, N. H., & Khalid, A. (2016). A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security*, *14*(1), 52.
3. Dartois, J. E., Knefati, A., Boukhobza, J., & Barais, O. (2018). Using quantile regression for reclaiming unused cloud resources while achieving sla. In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 89-98). IEEE.
4. Shahrad, M., & Wentzlaff, D. (2016). Availability knob: Flexible user-defined availability in the cloud. In Proceedings of the Seventh ACM Symposium on Cloud Computing (pp. 42-56).
5. Qanbari, S., Li, F., Dustdar, S., & Dai, T. S. (2014). Cloud Asset Pricing Tree (CAPT). In Proceedings of the 4th International Conference on Cloud Computing and Services Science (pp. 221-229). Barcelona, Spain. April.
6. Vázquez, C., Tomás, L., Moreno, G., & Tordsson, J. (2013). A fuzzy approach to cloud admission control for safe overbooking. In International Workshop on Fuzzy Logic and Applications (pp. 212-225). Springer, Cham.
7. Almutairi, A., Sarfraz, M. I., & Ghafoor, A. (2015). Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters. IEEE Transactions on Cloud Computing, 6(1), 168-181.
8. Jain, K., Mai, T., & Vazirani, V. V. (2017). A Performance-Based Scheme for Pricing Resources in the Cloud. In International Conference on Web and Internet Economics (pp. 281-293). Springer, Cham.
9. August, T., Niculescu, M. F., & Shin, H. (2014). Cloud implications on software network structure and security risks. Information Systems Research, 25(3), 489-510.
10. Nowicka, K. (2016). Cloud computing in sustainable mobility. Transportation Research Procedia, 14, 4070-4079.
11. Chang, V. (2016). Analyzing French and Italian iPhone 4S Mobile Cloud Customer Satisfaction Presented by Organizational Sustainability Modeling. In Web-Based Services: Concepts, Methodologies, Tools, and Applications (pp. 1068-1087). IGI Global.
12. Aminnezhad, A., Dehghantanha, A., Abdullah, M. T., & Damshenas, M. (2013). Cloud forensics issues and opportunities. International Journal of Information Processing and Management, 4(4), 76.

13. Chang, V. (2014). The big data analysis for measuring popularity in the mobile cloud. The first international workshop on Emerging Software as a Service and Analytics, ESaaSA
14. Zhang, F., & Gong, Z. (2021). Supply chain inventory collaborative management and information sharing mechanism based on cloud computing and 5G Internet of Things. Mathematical Problems in Engineering, 2021.
15. Kodym, O., Kubáč, L., & Kavka, L. (2020). Risks associated with Logistics 4.0 and their minimization using Blockchain. Open Engineering, 10(1), 74-85.
16. Wei, Q., Shao, H., & Zhang, G. (2018). Flexible, secure, and reliable data sharing service based on collaboration in multicloud environment. Wireless Communications and Mobile Computing, 2018.
17. Kamhoua, C., Martin, A., Tosh, D. K., Kwiat, K. A., Heitzenrater, C., & Sengupta, S. (2015). Cyber-threats information sharing in cloud computing: A game theoretic approach. In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 382-389). IEEE.
18. Koo, C. J., & Kim, J. (2015). Decision making for the adoption of cloud computing for sensor data: From the viewpoint of industrial security. International Journal of Distributed Sensor Networks, 11(9), 581563.
19. Islam, S., Mouratidis, H., & Weippl, E. R. (2013). A goal-driven risk management approach to support security and privacy analysis of cloud-based system. In Security Engineering for Cloud Computing: Approaches and Tools (pp. 97-122). IGI Global.
20. Rostek, K., Wiśniewski, M., & Kucharska, A. (2012). Cloud business intelligence for SMEs consortium. Foundations of Management, 4(1), 105-122.
21. Ayaburi, E. W. Y., Maasberg, M., & Lee, J. (2020). Decision Framework for Engaging Cloud-Based Big Data Analytics Vendors. Journal of Cases on Information Technology (JCIT), 22(4), 60-74.
22. Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of Urban Technology, 26(2), 47-65.
23. Horvath, R., Nedbal, D., & Stieninger, M. (2015). A literature review on challenges and effects of software defined networking. Procedia Computer Science, 64, 552-561.
24. Ghachem, F., Bennani, N., Ghedira, C., & Ghoddous, P. (2011). Towards a trust-manager service for hybrid clouds. In Web Information Systems Engineering–WISE 2011 and 2012 Workshops (pp. 70-76). Springer, Berlin, Heidelberg.

25. Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. International journal of information management, 33(5), 726-733.
26. Rabaey, M. (2012). A public economics approach to enabling enterprise architecture with the government cloud in Belgium. In Enterprise Architecture for Connected E-Government: Practices and Innovations (pp. 467-493). IGI Global.
27. Remondino, M. (2017) A Managerial Perspective of Technological Cloud Paradigms: its Effects on Enterprise Business, Costs and Strategies.
28. Wang, M., Zhu, L., & Zhang, Z. (2016). Risk-aware intermediate dataset backup strategy in cloud-based data intensive workflows. Future Generation Computer Systems, 55, 524-533.
29. Khan, A. M., Freitag, F., Gupta, S., Muntès-Mulero, V., Dominiak, J., & Matthews, P. (2015). On supporting service selection for collaborative multi-cloud ecosystems in community networks. In 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (pp. 634-641). IEEE.
30. Chou, Y., & Oetting, J. (2011). Risk assessment for cloud-based IT systems. International Journal of Grid and High Performance Computing (IJGHPC), 3(2), 1-13.
31. Marbukh, V. (2014). On systemic risk in the cloud computing model. In 2014 26th International Teletraffic Congress (ITC) (pp. 1-8). IEEE.
32. Kronabeter, A., & Fenz, S. (2012). Cloud security and privacy in the light of the 2012 EU data protection regulation. In International Conference on Cloud Computing (pp. 114-123). Springer, Cham.
33. Thomas, P. (2012). Harnessing the potential of cloud computing to transform higher education. In Cloud Computing for Teaching and Learning: Strategies for Design and Implementation (pp. 147-158). IGI Global.
34. Sabahi, F. (2011). Cloud computing security threats and responses. In *2011 IEEE 3rd International Conference on Communication Software and Networks* (pp. 245-249). IEEE.
35. Bulusu, S., & Sudia, K. (2013). A study on cloud computing security challenges.
36. Glassdoor. (2021). How much does a IT Specialist make? Retrieved 17 June, 2021, from https://www.glassdoor.com/Salaries/it-specialist-salary-SRCH_KO0,13.htm
37. Smith D. (2019). What's the Real Cost of Training Programs for Employees? Retrieved 17 June, 2021, from https://www.bizlibrary.com/blog/training-programs/cost-of-training-employees/#:~:text=In%20

2018%2C%20across%20all%20industries,%241%2C046%20per%20employee%20on%20training.

38. Long, M. R. (2020). The 5 Best Identity Management Software for Small Businesses. Retrieved 17 June, 2021, from https://www.fool.com/the-blueprint/identity-management/
39. Barclay Simpson. (2016). Calculating the reputational cost of cybersecurity breaches. Retrieved 17 June, 2021, from https://www.barclaysimpson.com/industrynews/calculating-the-reputational-cost-of-cybersecurity-breaches-801817323
40. Brook, C. (2020). What's the Cost of a Data Breach in 2019? Retrieved 17 June, 2021, from https://digitalguardian.com/blog/whats-cost-data-breach-2019
41. Glassdoor (2021). How much does a IT Specialist make? Retrieved 17 June, 2021, from https://www.glassdoor.com/Salaries/it-manager-salary-SRCH_KO0,10.htm
42. Prime Factors. (2017). Encryption: The Cost, The Protection, and the ROI. Retrieved 17 June, 2021, from, https://www.primefactors.com/resources/blog/encryption/encryption-the-cost-the-protection-and-the roi/#:~:text=The%20Ponemon%20Institute%20placed%20the,desktops%20and%20laptops%20at%20%24235.
43. Tunggal, A. T. (2021). What is the Cost of a Data Breach in 2021? Retrieved 17 June, 2021, from https://www.upguard.com/blog/cost-of-data-breach#:~:text=According%20to%20the%202019%20Cost,to%20%243.92%20million%20in%202020.
44. Trustradius. (n.d.). Data Loss Prevention Software Overview. Retrieved 17 June, 2021, from https://www.trustradius.com/data-loss-prevention#:~:text=Data%20loss%20prevention%20software%20is,start%20at%20about%205%2C000%20seats.