Communications in Mathematics and Applications
Vol. 13, No. 2, pp. 795–806, 2022
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v13i2.2032

http://www.rgnpublications.com

Review Article

Data Security Challenges and Solutions in Cloud Computing: Critical Review

Shuruq Zayed Al-Otaibi

Information Science Department, Arts Faculty, King Saud University, Prince Turkey St., Riyadh, Saudi Arabia
szalotaibi@ksu.edu.sa

Received: January 10, 2022 **Accepted:** February 21, 2022

Abstract. This paper was prepare, based on the sensitivity of data security topics, and based on the controversy surrounding cloud-computing security. Therefore, this paper aimed to contribute by providing some tips and directions related to cloud security through critical review for a number of recent studies. Then, extracting the most important latest problems and solutions that related to data security in cloud computing; and presenting them all in one study to become a comprehensive reference. The study found that the most important problems are data leakage, data remoteness, privacy and data segregation. As for the most important solutions that this paper reached to meet these challenges, were using practical strategies like models and standards, and using different emerging and programming technologies such as encryption, digital signatures, hashing, and blockchain, smart contracts, IoTs sensors and devices, edge computing, and fog computing. The study recommended researchers to conduct more theoretical and practical research on the subject, and recommended the cloud services providers to adopt several practical strategies and emerging technologies for higher protection.

Keywords. Cloud computing, Cloud security, Data security, Encryption, Cryptography

Mathematics Subject Classification (2020). 68Q01, 68M25, 14G50

1. Introduction

Cloud computing (CC) has started in the mid 90's, and one of its earlier providers are Amazon and Ali Baba, it is growing fast in the field of computer science [17]. NIST has defined CC as a model for enabling ubiquitous, convenient and on-demand network access to a shared pool –of configurable computing resources– that is provisioned and released rapidly with minimal management effort or service provider interaction [9]. In sum, CC is the newest web-based

computing network that offers the users with convenient and flexible resources to access or function with different cloud applications [18]. So, the main feature of this technology is that the user does not need to worry of any setup of costly computing infrastructure and that saves cost and time for any organization [13].

The CC model is composed of eight essential characteristics, which are on-demand self-service, broad network access,provisioning, scalability, measured service, location independence, cost effectiveness, and finally multi-tenancy. Moreover, there are three service models that are *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), and *Software as a Service* (SaaS) [6].

Due to the increasing growth of technologies and the diversity of user needs in the field of information technology, the position of CCis developing and growing very fast [4]. CC now-a-days is being used in many areas around the world. Although of CC many advantages, the transformation of local computing system to a virtual computing environment also brings many security challenges and issues with it for both parties the consumer and service provider [13]. These security issues ofCC brings much more challenging situations regarding data privacy, data protection, authenticated access etc. Due to these issues, adoption of CC is becoming difficult in today's era [12]. Especially in business, because the data situation is exceptionally important, and any data leaking or corruption can cause the collapse of that business. For that, this is one among the most reasons for cloud computing companies to offer more attention to data security [10], so it is important to tackle the security issues of CC before implementing it in an organization [18].

Based on all of the above, the researcher concluded the need to prepare a scientific comprehensive paper that aims to identify and gather the most important and latest issues and challenges that affect the subject of data security in CC in one paper, in addition, it aims to extract the best solutions and suggestions recently proposed during recent years. Where the researcher saw just a few studies that extensively addressed most of the information security challenges of CC, along with indicating to the solutions, all in just one study. Therefore, it is possible to formulate the study problem with the following main phrase:

What are the most important and recent challenges, and their solutions related to data security in the cloud-computing environment?

The researcher considered that the appropriate methodology for this paper is the critical review of the latest scientific studies in this field. So that, the most important solutions, proposals and recommendations that affect the problem of the current study can be extracted, with a focus on the strengths and weaknesses in these studies in order to better understand. Knowing that, this paper consists of six parts: introduction, article body, results, discussion and conclusion.

2. Reviews' Details

The used methodology in this paper is a critical review, which means a critical evaluation of a document (or book or chapter or article). It is not just a summary of the contents. It is achieved by reading, making judgments about the document and justifying these judgments [8].

The next section aims to present and critically review a number of studies related to the topic of challenges and solutions in the field of data security in CC. In addition, they will be arranged in descending chronological order from the newest to the oldest and then alphabetically based on the study title, which fall within the period 2017-2021, noting that the total number of studies that will be reviewed are 15 studies, distributed as follows:

Study [18] entitled: 'A Review of Data Security Challenges and their Solutions in Cloud Computing'

In this review study, the researchers gave attention to the data related security issues and solutions to be addressed in the CC network. Depending on the study, CC providers can protect the data from malicious users by implementing the following:
(1) Standard encryption whether this type of encryption is: homomorphic (enables for easy processing of the encrypted content), symmetric (requires a rudimentary cryptography, which facilitates protected search capabilities over sensitive data), or based on attribute(consists of either text security cipher or key code). (2) Heterogeneous data-centric authentication should be used for data access control.3-A designed blueprint for authentication. (4)The hash calculations for records integrity. (5) Testing the integrity of RSA-based data (can be done by merging identity based and RSA Signature cryptography) for data integrity.

The strength of this study lies in the list that explained different challenges of data security in cloud computing, and in the recommended techniques above for CC providers, and lies, also, in the listed models for each challenges, with explaining the effectiveness and limitations of each model.

Study [1] entitled 'A Model for Examining Challenges and Opportunities in Use of Cloud Computing for Health Information Systems'

This study proposed a detailed model in which can be employed by executive management of health organizations, especially senior clinical management positions, to make an informed decision on adoption of CC for Health Information Systems (HIS). The methodological strength of this study stems from the multiplicity of its methods including: the extensive review of the academic, extensive experience of one of the authors in this area, interviews with experts in healthcare informatics or cloud computing fields and stems from the multiplicity of its main and sub-hypotheses. The proposed model based on a rigorous research and has face validity, content validity, and nomological validity. Each of the dimensions outlined can be evaluated critically before the adoption decision. The study was also distinguished by listing the most important future research trends for the dimensions that affect cloud computing, including data security, and mentioned the most appropriate methodologies that can be implemented with this research. The study also focused on mentioning the most important technical trends that can address data problems in the cloud, such as blockchain technologies, smart contracts, wearable's and Internet of Things (IoT) sensors and devices as an efficient solutions for CC problems.

Study [10] entitled 'Analyzing Data Security Issues and Solutions in Cloud Computing'

This review paper discussed the various data security issues in CC during a multi-tenant environment and proposed methods to treat the safety issues. This paper also described CC models like the deployment models and therefore the service delivery models.

This study has classified data security problems into three sections, which are as follows: Security Challenges in the CIA Triad (Confidentiality, Integrity and Availability), Authentication and Access Control (AAC) and Security Challenges Due to Broken Authentication, Session and Access Controls.The study also indicated that, Cloud service Providers (CSPs) are responsible for the cloud infrastructure security and Cloud service Customers (CSCs) are responsible for the data and other things those are stored in the cloud. Therefore, security becomes a shared responsibility between CSP and CSC. For Example, Amazon Web Services (AWS), where both CSP and CSC share security responsibility and they called it as 'Shared Security Responsible Model'.

What gives this study importance is that it provided practical and implementable solutions and methods to overcome the previously mentioned data security problems.

Study [4] entitled 'A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining'

This paper is using a novel method to propose a hybrid model to give the user complete control over data protection in CC platform through data mining and decision tree algorithm.

The model presenting an innovation approach based on a combination of the decision tree method and cryptography through cryptographic protocols to define the authorized users or the unauthorized ones.

The great about this study is that it compared the proposed model with other methods and these comparisons showed that there are strengths on the customer side related to increasing the speed of access to and acquisition of cloud data, and considering the customer as the primary controller for access authentication by giving him control over encryption policies. On the other hand, there are many server-side weaknesses such as excessive file processing time on the server side, client dependency, and the server being considered a secondary entity that is not authorized to access and read data.

Study [2] entitled 'A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies'

This systematic literature review study aimed to review the existing research studies on CC security, threats, and challenges. This study examined the research studies published between 2010 and 2020 within the popular digital libraries. The study selected 80 papers to answer the proposed study questions. The outcomes of this study seven major security threats to CC services. The results showed that data tampering and leakage were among the highly security risks. Other identified security risks were associated with the data intrusion, data storage and data outsourcing in the CC environment remains a challenge for both cloud services providers (CSPs) and cloud users. The study identified the blockchain as a partnering technology to alleviate security concerns. Therefore, the study suggested CSPs, several strategies and practical approaches based on blockchain technologies frameworks to increase security in the cloud, so they can implement them. This study was also distinguished by its taxonomy that links each of the results of the study with its original reference from the studies.

Study [16] entitled 'Environment in Cloud Computing: Privacy Preservation and Security Solutions'

This review research is focusing on analyzing the CC security and privacy issues, and proposing a number of solutions and approaches to deal with these issues. The study touched on several approaches for preserving data privacy, such as the anonymity algorithm. The anonymity algorithm involves in processing the data by anonymizing few or all the data, to mine the specified knowledge from the cloud. This methodology differentiate from the classic cryptography technique by getting rid of key managing process, because of this reason it showcase as simple and flexible. Unfortunately, only finite number of services supported for this approach.

The study, also, touched on many methods for preserving security, one of them is the open guidelines and standards, which are basic for easy interoperable between the Applications programming interfaces inside the CSPs. Therefore, there are many open gauges are a work in progress; OGF's Open Cloud Computing Interface is one of them.

Study [5] entitled 'Risk Factors in Cloud Computing Relationships: A Study in Public Organizations in Sweden'

This research has looked to find the risk factors in CC relationships in public organizations in Sweden. A field survey methodology has been applied to this research, and the data has been collected through interviews with IT decision-makers with relevant experience in CC relationships, from five public organizations in Sweden were selected as participants in this study.

The study has identified security as a critical risk factor and has identified that uncertainty, caused by security, is the most important risk factor for building a good relationship between the service buyer and provider in the studied public organizations in Sweden. The Cloud computing clients do not trust their providers and therefore, they do not place sensitive data in the cloud. Additionally, the research have found other risks in CC that are not critical, like, asset specificity, a small number of suppliers, uncertainty, relatedness, measurement problems, competences. The main limitation in this research is low number of investigated public organizations in Sweden and therefore, the results could not be generalized. Therefore, in a future research is highly recommended to study the risks in CC relationships in other public organizations in Sweden.

Study [17] entitled 'Cloud computing security challenges'

This review study was characterized as it focused on identifying the most important risks facing CC, which are (virtualized services, centralized storage, multi-tenant access and security challenges). The study then explained the fourth factor, which is the security challenges, and it mentioned the most important of those challenges, which are (third party handing data, cyber-attack, insider attack, governmental intrusion, lack of support and lack of standardization).

This study was distinguished from the others studies in that it stated a fourth model for CC services called data as service DAAS, which is a customer software, that provide the user with data. However, what is missing from this study is that it did not refer to the solutions or even to the existence of those solutions.

Study [13] entitled 'Cloud Computing Security Challenges and its Potential Solution'

The aim of this survey is to provide a brief overview of CC technology, current and future trends of this technology, services provided by the CC and security issues and challenges.

The distinction of this study is that it proposed a system or method, to enhance the trust in CC and the confidentiality of the data by performing verification, authentication and encrypted data transmission. The proposed system is using an asymmetric cryptography depending on the RSA algorithm that using two different keys for more security, along with Digital Signature. The digital signature assurance that the authenticity of an electronic message or document is unmodified and original. Moreover, the study indicates a high probability that state-of art cryptographic mechanisms and electronic audit will play a vital role in cloud security and have much scope of work and research by academia. At the end, the study recommends researchers to conduct researches to address the security genuine issues of CC, mainly protection and security challenges of cloud data (cloud servers) and cloud consumer (cloud clients).

Study [3] entitled 'Edge Computing VS. Cloud Computing: Challenges And Opportunities In Industry 4.0'

This review research has focused on comparing these two technologies (cloud and edge computing) based on many comparison dimensions, including the dimension of network and data security. The study clarified and defined the challenges and opportunities in both of these

technologies by providing a better understanding what to use in practice. The importance of this study comes from the lack of literature reviews linking and comparing these two techniques.

The research has considered the CC challenges, the security of network and data represent the biggest obstacle of implementing this technology, since the location of data is outside the industrial environment. For that, the research has mentioned many practical trends of performing computing as close to the device as possible, relying on Edge Computing technologies, because Edge Computing offers more secure network and data transfer since it is placed inside the industry.

Based on this research, Cloud and Edge Computing will not replace each other, but rather complement each other, to achieve mutual benefit between them. Edge Computing provides solutions for difficulties in Cloud Computing and vice versa, and the combination of these two computing technologies have the ability to facing many data security threats.

Study [11] entitled 'Security and Privacy Issues in Cloud, Fog and Edge Computing'
In this review paper, the researchers analyzed the different privacy and security problems in three computing paradigms (cloud, fog, and edge computing), and proposed the suitable solutions for all paradigm separately.

The paper also noted that Internet of Things (IoT) is a continuously growing field. In addition, with increasing data and data generating devices in IoTs we will have to transfer from traditional computing techniques to new powerful techniques. In addition, as the number of data continues to grow, we should discover new computation techniques keeping in mind the security and the privacy of the user data first before anything else. For that, fog and edge computing have started replacing traditional cloud computing for computing the data that comes from IoTs devices.

Based on the foregoing, the paper recommended that edge and fog computing should replace traditional cloud computing as much as possible, and more research can be done to reduce the latency and the bandwidth requirement even further without compromising with the security of the system.

Study [12] entitled 'Security Issues in Cloud Computing and their Solutions: A Review'
This review study has been discussed various security issues regarding data privacy and reliability, key factors which are affecting the CC, and also solutions on particular areas, such as data security, have been proposed. One of the solutions that has proposed by the study to deal with data security was the encryption of data before sending it to the cloud, especially multi-stage encryption.In addition, the study indicated that there is experimental results show that RSA+IDEA gives the higher performance of encryption in securing the data.

The study also indicated to cope if there is Distributed Denial of service –a kind of attack that affecting the machines– by activating the use of a layer named as fog layer, which sits in between cloud server and user. So that, all the requests made to server are filtered through this fog layer and the attacks will be minimized. Digital signature was also proposed in this study as a powerful tool for securing data in CC. One example of such digital signatures is Prashant Rewagad model that is using digital signature to secure data along with Diffie Hellman key exchange with AES encryption algorithm.

Study [7] entitled 'The Proposed Model to Increase Security of Sensitive Data in Cloud Computing'
The aim of this study is to propose a model to control data security in the cloud. The proposed model offers three scenarios based on the data sensitivity. The first scenario applies in the

case of sensitive data, which uses asymmetric algorithms because it is the safest. The second scenario applies in the case of moderate level of data security, which uses hybrid algorithms. The third scenario applies in the case of least sensitive data, which uses symmetric algorithms because it is the least safe, but it is the fastest on the other hand.

The study, also, proposed schemas that are used as measurements for the used algorithms in the model. The strength of this study lies in its multiple scenarios and schemas' measurements to deal with the degree of sensitivity of the data.

Study [15] entitled 'Cloud Computing: Security Issues & Solution'

The study revealed that the major factor in cloud security issues is data security, especially data integrity, data Privacy & confidentiality,data availability and data location & relocation

Therefore, the study proposed a hybrid algorithms approach that consists of RSA and SHA1, trying to meet the objective of data security. The purpose of merging these two specific algorithms together is the ability of the RSA for encryption and SHA1 for hashing. Where this approach is based on, taking a string that comes from client to the cloud and then generating the public key and private key, and encrypting the string using the RSA algorithm and finally generating the hash value of the same message using SHA1.

The distinction in this study is that it explained the proposed method of work in a detailed, accurate and systematic manner.

Study [14] entitled 'Security Issues and Solutions in Cloud Computing'

This review paper attempted to describe the Security challenges in the application and data security at SaaS. Therefore, the paper purpose was to provide a security perspective of SaaS service, and to resolve that issue.

The study reported that the best method to assess a SaaS vendor's privacy and security measures is through the use of third-party certification procedures. One of the most relevant certification, known as ISO 27001, which provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information-security management system.

The study also clarified that Cryptography is a widely used technique, which is reliable for data security. On the other hand, it will increase the cost of computation and it is technically weighty to process the data in an encrypted form. The proposed method to guarantee the privacy of data hosted on servers in the cloud is by encrypting and compressing the data in multi-server. This method deals with the compression and encrypts the data before it is taken as a backup in multi-server Using hybrid cryptography (a combination of asymmetric and symmetric cryptographic), to harness the efficiency of symmetric cryptography while maintaining the security of asymmetric cryptography.

3. Results

By presenting previous studies, and then presenting the most important issues and solutions related to information security in cloud computing, as well as by reviewing the most important strengths and weaknesses of those studies; the researcher reached the following results:

- The studies [1], [5] and [6] was characterized by their applied methodologies, where [1] and [5] used Field survey methodology in specific sectors (health and public organizations), while [6] used programming method by NET Framework 4.5 and C# language.
- The [12] and [18] studies agreed that prevention of data leakage is regarded to be the most common critical problem with percentage 88% of the major challenges in CC. On the other

hand, they disagreed on the other greatest data security problem with percentage 92% of major challenges; where [18] indicated that, it is represented in data remoteness and privacy. While [12] indicated that, it is represented in data segregation. Moreover, [12] was distinguished by presenting a detailed outline of the most important data security problems, with an explanation of their percentages, as follows in Figure 1:

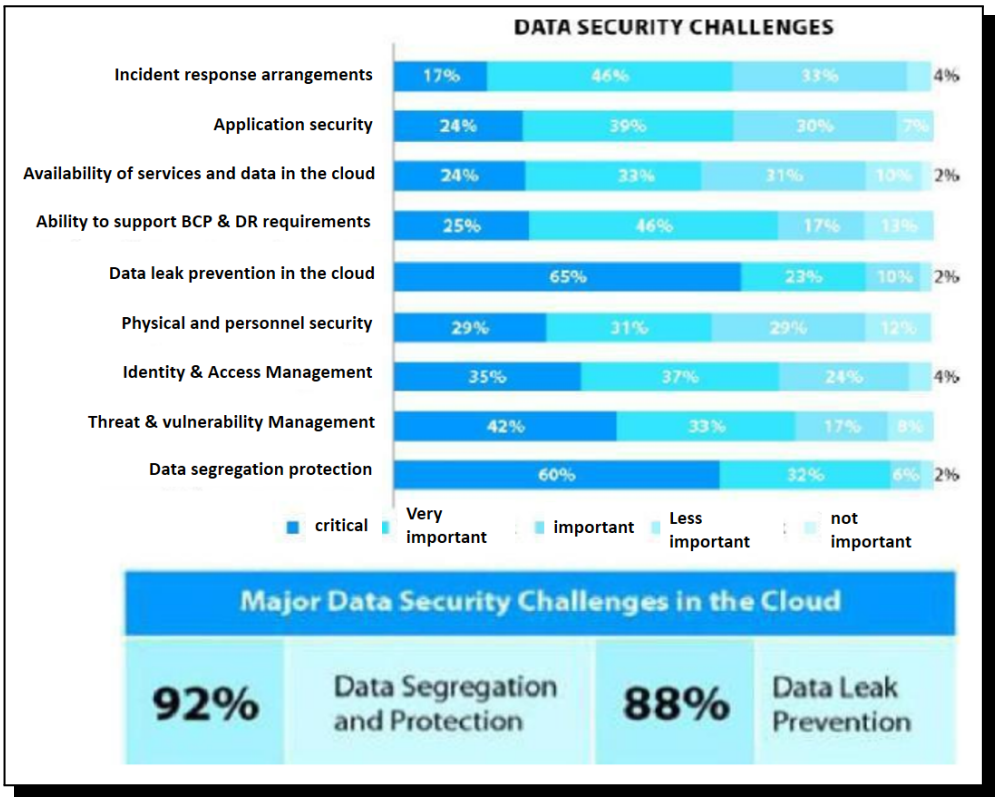

Figure 1. Data security challenges (study [12, p. 345])

- The [2] and [1] studies agreed that the use of blockchain technologies with CC alleviates data security problems. In addition, the [1] study added other useful emerging technologies in this aspect, namely:smart contracts, wearables and Internet of Things (IoT) sensors and devices.
- The study [10] has raised an important point as recommendation, which is that there are new developments in CC, such as: Container-as-a Service (CaaS), Software-defined networking, Software-defined-storage and Cloud-of-Things (CoT). Also, the study [17] has indicated there is new developments in CC called Data-as-a Service (DaaS). Therefore, all these new developments bring new challenges in CC and they need to be solved.
- The [3] and [11] studies disagreed regarding edge and fog computing, where [11] stated that it would replace CC in order to get rid of its problems, while [3] stated that edge computing would not replace CC but would complement each other in order to solve data security problems. In addition, the study [12] agreed with [3] about the necessity of having a fog layer in the middle between the user and the cloud server to prevent security problems such as attackers without getting rid of cloud services.

- Study [1] have the distinction of presenting the most important research trends in the field of cloud data security, and their best appropriate methodologies to be implemented as an effective solutions.
- Study [13] have the distinction of referring to that electronic audit will play a vital role in cloud security and will have much scope of work and research by academia, and also was distinguished by clarifying the security architecture in each layer of the cloud as follows in Figure 2:

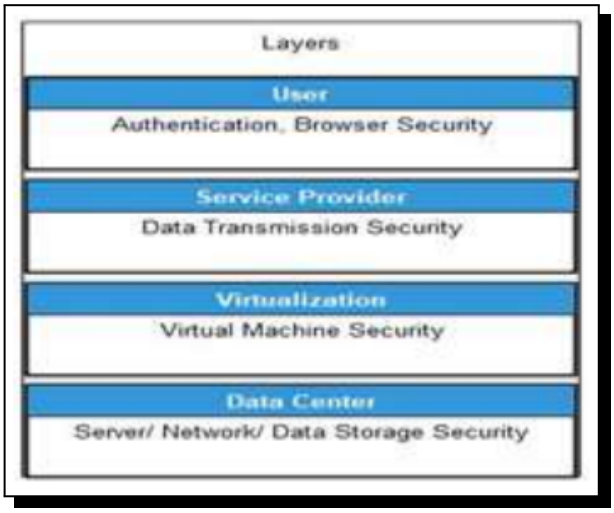

Figure 2. Security architecture of cloud layers (study [13, p. 171])

- Some of the studies have suggested detailed practical strategies for solving data security problems in the cloud, as follows:
  - *Models*: such as studies [1, 4, 7, 18].
  - *Methods or approaches*: such as studies [2, 12–16, 18].
  - *Tips*: such as studies [3, 10, 11].
  - *Standards*: such as OGF's in study [16] and ISO 27001in study [14].
- Several studies above have recommended the use of special technical and programming solutions in order to address data security challenges, as follows:
  - *Encryption and Cryptography:* such as studies [1, 4, 7, 10, 12, 13]. These studies also mentioned various types of encryption and cryptography such as homomorphic, symmetric, asymmetric, multi-stage and hybrid encryption. Each type of all the previous ones has its pros and cons.
  - *Digital Signature:* such as studies [12, 13, 18].
  - *Hashing*: such as [15] and [18].
  - *Compression*: such as study [14].
  - *Specific Algorithms*: Such as RSA algorithm in studies [12, 13, 15, 18], decision tree algorithm in study [4], the anonymity algorithm in study [16], IDEA, AES algorithms in study [12], and SHA1 in study [15].

- The current study shares with previous studies that they all aim to identify the most important security issues and problems facing data in the CC environment, and they all – except for study [17] – aim also to find the most important and prominent solutions to these issues and problems. Moreover, the current study is characterized by being keen on presenting the latest scientific studies related to the subject, which are located between the period (2017 until now), and is characterized, also, by a critical review methodology that shows the strengths and weaknesses of previous studies.

4. Discussion

After presenting the results related to the presentation of previous studies, and related to the review of the most important strengths and weaknesses of those studies; the following pivotal points can be drawn:

- CC has many distinct advantages and services, but in return, it faces several problems and security challenges, and one of the most important of these challenges is data security.
- Data leakage is considered to be the most common security critical problem, with percentage 88% of major problems in CC. Followed by, data remoteness, privacy, data segregation, vulnerability management and access management.
- The results showed that there are wide ranges of practical strategies that can be used as solutions such as models, methods, sequential steps, and standards.
- The previously mentioned practical strategies as solutions include many programming techniques, such as encryption and cryptography, hashing, digital signature, compression and algorithms.
- There are modern technologies that can be used in parallel with CC in order to reduce its security problems such as edge and fog computing, blockchain technologies, smart contracts, wearable's and Internet of Things (IoT) sensors and devices.
- There are new developments in CC, such as Container-as-a Service (CaaS), Data-as-a Service (DaaS), Software-defined networking, Software-defined-storage and Cloud-of-Things. Therefore, all these new developments bring new challenges in CC and they need to be solved.
- Academic and scientific research has a great role in providing solutions to data security problems in CC.

5. Conclusion

Based on the previously proposed solutions, which range from technical and programming solutions, practical strategies, research trends, and emerging technologies; the researcher recommends the following persons:

- Researchers and academics to conducting several scientific research (theoretical and practical) in the field of cloud computing data security.
- CSPs to adopt emerging technologies that work collaboratively with the cloud in order to mitigate cloud security problems, as well as adopting several methods and techniques for high protection.
- Organizations and users to choose CSPs carefully after reviewing their security strategy and customer experiences.

Acknowledgements

All thanks to King Saud University, which supported this research until it appeared in this final form.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] A. Al-Marsy, P. Chaudhary and J.A. Rodger, A model for examining challenges and opportunities in use of cloud computing for health information systems, *Applied System Innovation* **4** (2021), 15, DOI: 10.3390/asi4010015.

[2] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, A systematic literature review on cloud computing security: threats and mitigation strategies, *IEEE Access* **9** (2021), 57792 – 57807, DOI: 10.1109/ACCESS.2021.3073203.

[3] B. Bajic, I. Cosic, B. Katalinic, S. Moraca, M. Lazarevic and A. Rikalovic, Edge computing vs. cloud computing: challenges and opportunities in industry 4.0, in *Proceedings of the 30th DAAAM International Symposium*, B. Katalinic (Ed.), pp. 0864 – 0871, (2019), DAAAM International, Vienna, Austria, DOI: 10.2507/30th.daaam.proceedings.120.

[4] Q. He and H. He, A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining, *Sustainability* **13** (2021), 101, DOI: 10.3390/su13010101.

[5] G. Hodosia, A. Haiderb and L. Rusu, Risk factors in cloud computing relationships: a study in public organizations in Sweden, *Procedia Computer Science* **181** (2021), 1179 – 1186, DOI: 10.1016/j.procs.2021.01.315.

[6] J. Hurwitz, M. Kaufman and G. Hapler, *Cloud Services for Dummies*, John Wiley & Sons, Inc., New Jersey (2012), URL: https://www.ibm.com/cloud-computing/files/cloud-for-dummies.pdf.

[7] D. Hyseni, B. Selimi, A. Luma and B. Cico, The proposed model to increase security of sensitive data in cloud computing, *International Journal of Advanced Computer Science and Applications* **9**(2) (2018), 203 – 210, DOI: 10.14569/IJACSA.2018.090229.

[8] Learning Experience Team, *Writing a Critical Review*, Learning Zone, Southern Cross University, (2020), available at: https://www.scu.edu.au/media/scueduau/staff/teaching-and-learning/talking-teaching/writing_a_critical_review.pdf.

[9] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology (NIST), (2011), available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

[10] R. Nivetha and S.I. Shyla, Analyzing data security issues and solutions in cloud computing, *International Journal of Advanced Research in Science, Communication and Technology* **2**(1) (2021), 49 – 55, URL: https://ijarsct.co.in/Paper752.pdf.

[11] S. Parikh, D. Dave, R. Patel and N. Doshi, Security and privacy issues in cloud, fog and edge computing, *Procedia Computer Science* **160** (2019), 734 – 739, DOI: 10.1016/j.procs.2019.11.018.

[12] S. Sabir, Security issues in cloud computing and their solutions: a review, *International Journal of Advanced Computer Science and Applications* **9**(11) (2018), 343 – 346, DOI: 10.14569/IJACSA.2018.091147.

[13] A.W. Salehi, F. Noori and R. Saboori, Cloud computing security challenges and its potential solution, *American Journal of Engineering Research* **8**(10) (2019), 165 – 175, URL: https://www.ajer.org/papers/Vol-8-issue-10/S0810165175.pdf.

[14] A.K. Sen and P.K. Tiwari, Security issues and solutions in cloud computing, *IOSR Journal of Computer Engineering* **19**(2) (2017), 67 – 72, DOI: 10.9790/0661-1902046772.

[15] S. Singh, T. Nafis and A. Sethi, Cloud computing: security issues & solution, *International Journal of Computational Intelligence* **13**(6) (2017), 1419 – 1429.

[16] J. Sumitha, V. Padmaja and R. Vaishnidi, Environment in cloud computing: privacy preservation and security solutions, *International Journal of Scientific Research and Engineering Development* **4**(2) (2021), 1129 – 1133, URL: http://www.ijsred.com/volume4/issue2/IJSRED-V4I2P146.pdf.

[17] N.R. Tadapaneni, Cloud computing security challenges, *International Journal of Innovations in Engineering Research and Technology* **7**(6) (2020), 5 pages, URL: https://repo.ijiert.org/index.php/ijiert/article/view/306/285.

[18] I. Zulifqar, S. Anayat and I. Kharal, A review of data security challenges and their solutions in cloud computing, *International Journal of Information Engineering and Electronic Business* **13**(3) (2021), 30 – 38, DOI: 10.5815/ijieeb.2021.03.04.