International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 26 August 2023 **Revised:** 10 October 2023 **Accepted:** 25 October 2023*

A Study on Data Protection in Cloud Environment

Dr. S Arvind[1], Dr. Siva Shankar S[2], Dr. D. Hemanand[3], Dr. C. Ashok Kumar[4], G. Nagarjuna Rao[5]
[1]Professor, Department of Computer Science Engineering Hyderabad Institute of Technology and Management Mail :scarvi@rediffmail.com
[2]Associate Professor & Dean Foreign Affairs Department of CSE KG Reddy College of Engineering and Technology Chilukuru village Hyderabad -501504 Mail : drsivashankars@gmail.com
[3]Professor,Department of Computer Science and Engineering,S.A. Engineering College Poonamallee-Avadi Road, Thiruverkadu, Chennai-600077 Tamil Nadu, India
Mail : hemanand1982@gmail.com
[4]Assistant Professor,Department of Computing Technologies,School of Computing,SRM Institute of Science and Technology,Kattankulathur, Chennai-603203 9894331626/8610805769.
Mail: ashokkuc@srmist.edu.in
[5]Assistant Professor Department of CSE MLR Institute of Technology, Dundigal, Hyderabad
Mail : nagarjunarao.gudelli@gmail.com

Abstract

Data protection in the online environment pertains to the safeguarding of sensitive or important data kept, analyzed, or sent in cloud-based systems. It entails assuring data confidentiality, integrity, and availability, as well as adhering to appropriate data protection requirements. In a nutshell, cloud data protection seeks to protect data against unauthorized access, deletion, or breaches while retaining its accuracy and accessible to authorized users. This is accomplished in the cloud environment using various security measures, encryption approaches, access controls, disaster recovery and backup processes, and constant monitoring and threat detection. The research significance of data protection in the cloud environment can be summarized as follows: Security and Privacy: Research in data protection in the cloud helps address the security and privacy concerns associated with storing and processing sensitive data in cloud-based systems. It explores and develops advanced security mechanisms, encryption techniques, and access controls to protect data from unauthorized access, data breaches, and privacy violations. Trust and Confidence: Research in data protection contributes to building trust and confidence in cloud computing. By developing robust security solutions and demonstrating their effectiveness, research helps alleviate concerns about data security and privacy, fostering greater adoption of cloud services by organizations and individuals. Compliance and Regulations: Cloud computing often involves compliance with data protection regulations and industry standards. Research in this area explores the legal and regulatory aspects of data protection in the cloud and helps organizations understand and comply with relevant requirements. Data Resilience and Recovery: Research in data protection focuses on ensuring data resilience and developing efficient data recovery mechanisms in the cloud. It explores backup and disaster recovery strategies, data replication techniques, and data loss prevention methods to minimize downtime, recover data promptly, and maintain business continuity in the event of system failures or disasters. By addressing these research areas, studies on data protection in the cloud environment contribute to enhancing security, privacy, compliance, and resilience in cloud computing. They provide valuable insights, practical solutions, and guidelines for organizations and service providers to protect data effectively and maintain the trust of users in cloud-based services. The weighted product method approach is commonly used to choose the best data protection in cloud environment. CCSS1, CCSS2, CCSS3, CCSS4, CCSS5 data visibility, data integrity, Maintains compliance, Data security, Data storage. From the result it is seen that CCSS2 got highest rank whereas CCSS5 got lowest rank According to the results, CCSS2 was ranked first.

Keywords: data visibility, data integrity, Maintains compliance, Data security, Data storage.

1. INTRODUCTION

Since the birth of IT-supported company management, the internet has been the most common method of providing software alternatives for consumers and employees. Client-server architectures were used. As a result, the applying company hosts the servers and networks in-house. Secure safeguarding information is a major, but manageable, concern in this technological approach. Cloud Computing technologies are now powering an expanding number of software applications. That is, the provider hosts the system's supporting hardware, and users gain permission to use the solutions via the Internet.

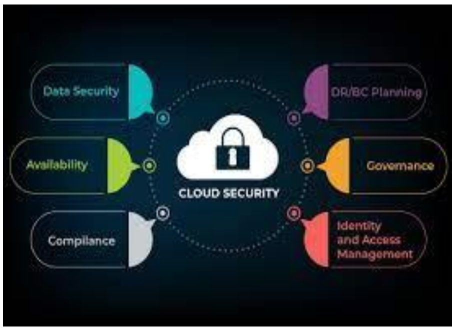

FIGURE 1. Cloud security

Cloud Computing offerings might vary depending on the specification (for example, platforms or infrastructure). The delivery of ready-to-use programmes based on this technological approach is referred to as Software with a Service (SAAS). Because Cloud Computing enables highly accessible, dynamic, and reliable IT services, this method of IT buying has increased interest for this solution. Although the total amount of cloud computing customers is continually expanding, several constraints continue to impede the method's widespread adoption, such as technical requirements such as scalability or, more specifically, legal considerations such as safeguarding information and privacy. The dispersed storing of data on other computers is one of the fundamental concepts of Cloud Computing. Aside from worries about potential data loss or theft, many consumers are unsure about the applicable legal requirements for privacy and security of data in this setting.

2. MATERIALS AND METHOD

Data visibility: The ability to obtain, view, and interpret data within an organisation or system is referred to as data visibility. It entails giving authorised users the tools and permissions they need to effectively visualise and comprehend data. In a nutshell, data visibility is the ability to view and understand data, allowing users to make educated decisions, find trends, and get insights from the data at their disposal.[6]

Data integrity: The quality, consistency, and dependability of data during its lifecycle is referred to as data integrity. It assures that data remains untouched and unaltered, devoid of errors, unauthorised changes, or corruption. In a nutshell, data integrity is the assurance that the information is accurate, comprehensive, and dependable, preserving its quality and dependability for successful decision-making and operational procedures.[8]

Maintains compliance: The process of conforming to applicable rules, regulations, as well as industry standards inside an organization is referred to as maintaining compliance. It entails making certain that the corporation's operations, processes, and practices are in accordance with the legal and regulatory regulations that govern its industry or sector. In a nutshell, compliance is the continual Endeavour to meet legal and regulatory duties in order to prevent penalties, legal challenges, and reputational damage whilst promoting responsible and ethical corporate practises.[10]

Data security: The protection protecting digital data from unauthorised access, use, openness, alteration, or destruction is referred to as data security. It entails putting in place numerous safeguards, rules, and practises to protect data and keep the information from falling into inappropriate hands or becoming compromised. In a nutshell, data security is the use of encrypting it restricted access, identification, restore and backup systems, and other precautions to secure the privacy, integrity, and accessibility of sensitive and essential data.[11]

Data storage: The practise of storing electronic information in an appropriately structured and easily accessible manner towards future use is referred to as data storage. It entails acquiring, organising, and storing data in a secure and dependable manner to assure its availability when required. In a nutshell, data storage is the systematic and effective management of data to allow for easy retrieval, effective processing, and preservation over the years. whichever fits the organization's needs and data management plans, this can be accomplished using a variety of storage technologies that include hard disc drives, solid-state devices, cloud storage, even tape storage.[12]

Weighted Product Method: The weighted product method (WPM) constitutes a multi-criteria decision-making strategy that evaluates and ranks alternatives depending on how well they perform across various criteria. It entails giving each criterion a weight to indicate its relative relevance and then generating an overall score for each choice through dividing the result's rating for each condition by the appropriate weight. In a nutshell, the weighted product technique is a mathematical strategy to determining the general order of alternatives in a process of choice-making by combining the weighted scores for criteria.[23]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *26 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *25 October 2023*

3. RESULT AND DESCUSSION

TABLE 1. Evaluation of Cloud Computing Security Software

	data visibility	data integrity	Maintains compliance	data security	data storage
CCSS1	4	5	7	5	5
CCSS2	8	7	6	5	6
CCSS3	8	3	7	9	3
CCSS4	4	4	4	6	9
CCSS5	3	6	4	3	7

Table 1 represents an evaluation of Cloud Computing Security Software (CCSS) based on different criteria. Each CCSS is assigned a score ranging from 1 to 10 for the following categories: data visibility, data integrity, maintenance of compliance, data security, and data storage. CCSS1 has a score of 4 for data visibility, 5 for data integrity, 7 for maintaining compliance, 5 for data security, and 5 for data storage. CCSS2 has a score of 8 for data visibility, 7 for data integrity, 6 for maintaining compliance, 5 for data security, and 6 for data storage. CCSS3 has a score of 8 for data visibility, 3 for data integrity, 7 for maintaining compliance, 9 for data security, and 3 for data storage. CCSS4 has a score of 4 for data visibility, 4 for data integrity, 4 for maintaining compliance, 6 for data security, and 9 for data storage. CCSS5 has a score of 3 for data visibility, 6 for data integrity, 4 for maintaining compliance, 3 for data security, and 7 for data storage. These scores represent the evaluated performance or effectiveness of each CCSS in the specified categories. Higher scores generally indicate better performance or stronger capabilities in that particular category.

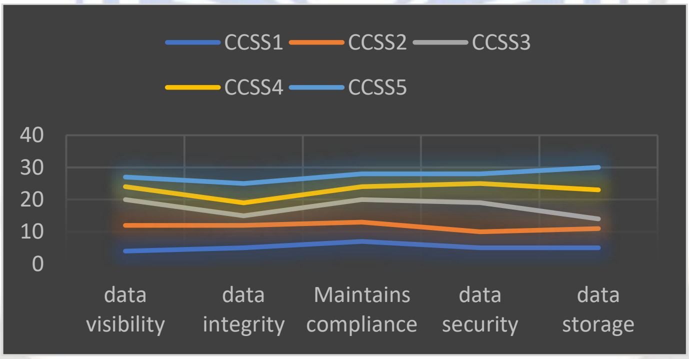

FIGURE 1. Evaluation of Cloud Computing Security Software

Figure 1 shows the graphical representation of an evaluation of Cloud Computing Security Software (CCSS) based on different criteria. Each CCSS is assigned a score ranging from 1 to 10 for the following categories: data visibility, data integrity, maintenance of compliance, data security, and data storage. CCSS1 has a score of 4 for data visibility, 5 for data integrity, 7 for maintaining compliance, 5 for data security, and 5 for data storage. CCSS2 has a score of 8 for data visibility, 7 for data integrity, 6 for maintaining compliance, 5 for data security, and 6 for data storage. CCSS3 has a score of 8 for data visibility, 3 for data integrity, 7 for maintaining compliance, 9 for data security, and 3 for data storage. CCSS4 has a score of 4 for data visibility, 4 for data integrity, 4 for maintaining compliance, 6 for data security, and 9 for data storage. CCSS5 has a score of 3 for data visibility, 6 for data integrity, 4 for maintaining compliance, 3 for data security, and 7 for data storage. These scores represent the evaluated performance or effectiveness of each CCSS in the specified categories. Higher scores generally indicate better performance or stronger capabilities in that particular category.

TABLE 2. Normalized matrix

CCSS1	0.50000	0.71429	1.00000	0.55556	0.55556
CCSS2	1.00000	1.00000	0.85714	0.55556	0.66667
CCSS3	1.00000	0.42857	1.00000	1.00000	0.33333
CCSS4	0.50000	0.57143	0.57143	0.66667	1.00000

CCSS5	0.37500	0.85714	0.57143	0.33333	0.77778

Table 2 shows the normalized matrix value of data set for evaluation of Cloud Computing Security Software. This is calculated according to the Weighted product method.

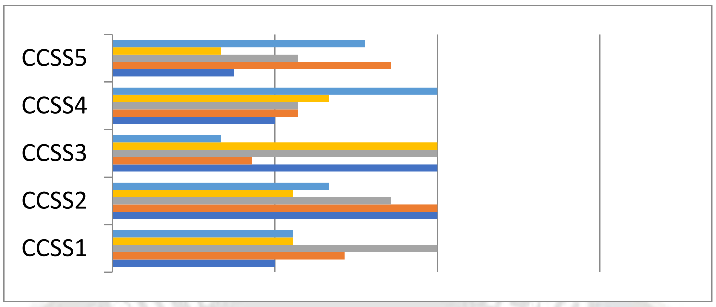

FIGURE 2. Normalized matrix

Figure 2 shows the normalized matrix value of data set for evaluation of Cloud Computing Security Software. This is calculated according to the Weighted product method.

TABLE 3. Weighted normalized decision matrix.

CCSS1	0.87055	0.93492	1.00000	0.88909	0.88909
CCSS2	1.00000	1.00000	0.96964	0.88909	0.92211
CCSS3	1.00000	0.84412	1.00000	1.00000	0.80274
CCSS4	0.87055	0.89411	0.89411	0.92211	1.00000
CCSS5	0.82188	0.96964	0.89411	0.80274	0.95098

Table 3 shows the weighted normalized matrix value of data set for evaluation of Cloud Computing Security Software. This is calculated according to the Weighted product method by multiplying weight matrix and normalized matrix.

TABLE 4. RANK

Cloud Computing Security Software	**Preference Score**	**WASPAS Coefficient**	**RANK**
CCSS1	0.643368	0.643368	3
CCSS2	0.794946	0.794946	1
CCSS3	0.677611	0.677611	2
CCSS4	0.641742	0.641742	4
CCSS5	0.543946	0.543946	5

Table 4 provides information about different Cloud Computing Security Software (CCSS) options, along with their preference scores, WASPAS coefficients, and ranks. CCSS1 has a preference score of 0.643368, a WASPAS coefficient of 0.643368, and is ranked 3rd. CCSS2 has the highest preference score of 0.794946, the highest WASPAS coefficient of 0.794946, and is ranked 1st. CCSS3 has a preference score of 0.677611, a WASPAS coefficient of 0.677611, and is ranked 2nd. CCSS4 has a preference score of 0.641742, a WASPAS coefficient of 0.641742, and is ranked 4th. CCSS5 has the lowest preference score of 0.543946, the lowest WASPAS coefficient of 0.543946, and is ranked 5th. Based on these scores and ranks, CCSS2 appears to be the most preferred cloud computing security software option, followed by CCSS3, CCSS1, CCSS4, and CCSS5.

***Article Received:** 26 August 2023 **Revised:** 10 October 2023 **Accepted:** 25 October 2023*

FIGURE 4

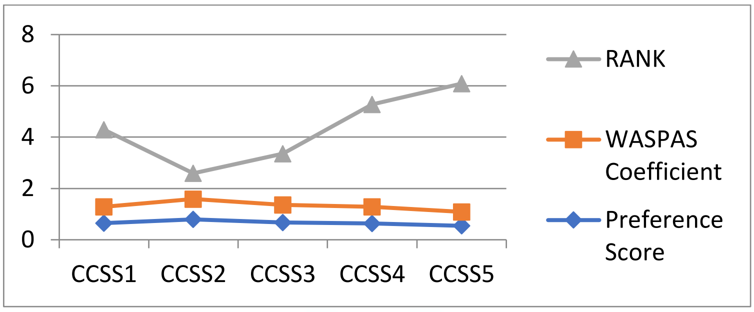

Figure 3 shows the graphical representation of the different Cloud Computing Security Software (CCSS) options, along with their preference scores, WASPAS coefficients, and ranks. CCSS1 has a preference score of 0.643368, a WASPAS coefficient of 0.643368, and is ranked 3rd. CCSS2 has the highest preference score of 0.794946, the highest WASPAS coefficient of 0.794946, and is ranked 1st. CCSS3 has a preference score of 0.677611, a WASPAS coefficient of 0.677611, and is ranked 2nd. CCSS4 has a preference score of 0.641742, a WASPAS coefficient of 0.641742, and is ranked 4th. CCSS5 has the lowest preference score of 0.543946, the lowest WASPAS coefficient of 0.543946, and is ranked 5th. Based on these scores and ranks, CCSS2 appears to be the most preferred cloud computing security software option, followed by CCSS3, CCSS1, CCSS4, and CCSS5.

CONCLUSION

The purpose of this study was to conduct a review of the current academic literature on contemporary cloud computing security mechanisms. The issues stemming from the implementation of these regulations. We concentrated on data transmission between the economies of the United States and the European Union because an examination The entity for international law would fall outside the scope for this article and would be impractical owing to space limits. Despite the fact that data security is one of the most significant factors of cloud computing clients, our examination of 33 studies discovered a lack of transparency and neglect within the academic literature. However, after the first draught of a general privacy regulation was published in 2012, there was an upsurge in the number of articles covering this delicate topic. Numerous findings emerged from our content analysis. Prospective studies in this area will face hurdles. Many academics criticise the large disparity in data. Protection laws among the United States and the European Union. However, there are few concrete examples in literature. A careful examination and contrast of the unique IT law for both countries would enable an assessment of the gaps in present legislation and the development of proposals to improve the situation. The same is true for assertions about the current regulations' inability to be directly applied to Cloud technologies: Our literature source did not provide detailed replies to why existing confidentiality agreements were not applicable to these solutions.

REFERENCES

[1]. Vu, Quang Hieu, Maurizio Colombo, Rasool Asal, Ali Sajjad, Fadi Ali El-Moussa, and Theo Dimitrakos. "Secure cloud storage: a framework for data protection as a service in the multi-cloud environment." In *2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 638-642. IEEE, 2015.

[2]. Pfarr, Florian, Thomas Buckel, and Axel Winkelmann. "Cloud Computing Data Protection--A Literature Review and Analysis." In *2014 47th Hawaii International Conference on System Sciences*, pp. 5018-5027. IEEE, 2014.

[3]. Hachim, Ethar Abdul Wahhab, Thekra Abbas, and Methaq Talib Gaata. "Modified RC4 Algorithm for Improve Data Protection in Cloud Environment." In *2022 International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 295-299. IEEE, 2022.

[4]. Chen, Lingfeng, and Doan Hoang. "Active data-centric framework for data protection in cloud environment." (2012).

[5]. Colombo, Maurizio, Rasool Asal, Quang Hieu Hieu, Fadi Ali El-Moussa, Ali Sajjad, and Theo Dimitrakos. "Data protection as a service in the multi-cloud environment." In *2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*, pp. 81-85. IEEE, 2019.

[6]. Chen, Lingfeng, and Doan B. Hoang. "Novel data protection model in healthcare cloud." In *2011 IEEE International Conference on High Performance Computing and Communications*, pp. 550-555. IEEE, 2011.

[7]. Fan, Kefeng, Xiangzhen Yao, Xiaohe Fan, Yong Wang, and Mingjie Chen. "A new usage control protocol for data protection of cloud environment." *EURASIP Journal on Information Security* 2016 (2016): 1-7.

[8]. Moghaddam, Faraz Fatemi, Mostafa Vala, Mohammad Ahmadi, Touraj Khodadadi, and Kasra Madadipouya. "A reliable data protection model based on re-encryption concepts in cloud environments." In *2015 IEEE 6th control and system graduate research colloquium (ICSGRC)*, pp. 11-16. IEEE, 2015.

[9]. Kim, Su-Hyun, and Im-Yeong Lee, eds. "Study on user authority management for safe data protection in cloud computing environments." *Symmetry* 7, no. 1 (2015): 269-283.

[10]. Moghaddam, Faraz Fatemi, Moslem Yezdanpanah, Touraj Khodadadi, Mohammad Ahmadi, and Mohammad Eslami. "VDCI: Variable data classification index to ensure data protection in cloud computing environments." In *2014 IEEE Conference on Systems, Process and Control (ICSPC 2014)*, pp. 53-57. IEEE, 2014.

[11]. Qiu, Han, Hassan Noura, Meikang Qiu, Zhong Ming, and Gerard Memmi. "A user-centric data protection method for cloud storage based on invertible DWT." *IEEE Transactions on Cloud Computing* 9, no. 4 (2019): 1293-1304.

[12]. Alnemr, Rehab, Erdal Cayirci, Lorenzo Dalla Corte, Alexandr Garaga, Ronald Leenes, Rodney Mhungu, Siani Pearson et al. "A data protection impact assessment methodology for cloud." In *Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, Revised Selected Papers 3*, pp. 60-92. Springer International Publishing, 2016.

[13]. Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)." *Information* 11, no. 12 (2020): 586.

[14]. Ismail, Noriswadi. "Cursing the cloud (or) controlling the cloud?." *Computer law & Security review* 27, no. 3 (2011): 250-257.

[15]. San Cristóbal Mateo, José Ramón, and José Ramón San Cristóbal Mateo. "Weighted sum method and weighted product method." *Multi criteria analysis in the renewable energy industry* (2012): 19-22.

[16]. Khairina, Dyna Marisa, Muhammad Reski Asrian, and Heliza Rahmania Hatta. "Decision support system for new employee recruitment using weighted product method." In *2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, pp. 297-301. IEEE, 2016.

[17]. Wang, Mingxi, Shulin Liu, Shouyang Wang, and Kin Keung Lai. "A weighted product method for bidding strategies in multi-attribute auctions." *Journal of Systems Science and Complexity* 23, no. 1 (2010): 194-208.

[18]. Ahsan, M., and N. Indawati. "Implementation weighted product method to determine multiple intelligence child." In *Journal of Physics: Conference Series*, vol. 1375, no. 1, p. 012038. IOP Publishing, 2019.

[19]. Supriyono, Heru, and Chintya Purnama Sari. "Developing decision support systems using the weighted product method for house selection." In *AIP Conference Proceedings*, vol. 1977, no. 1, p. 020049. AIP Publishing LLC, 2018.

[20]. Fitriasari, Novi Sofia, Syifa Afifah Fitriani, and Rosa Ariani Sukamto. "Comparison of weighted product method and technique for order preference by similarity to ideal solution method: Complexity and accuracy." In *2017 3rd International Conference on Science in Information Technology (ICSITech)*, pp. 453-458. IEEE, 2017.

[21]. Boltürk, Eda, Ali Karaşan, and Cengiz Kahraman. "Simple additive weighting and weighted product methods using neutrosophic sets." *Fuzzy multi-criteria decision-making using neutrosophic sets* (2019): 647-676.

[22]. Nababan, Labuan, and Elida Tuti. "Determination Feasibility of Poor Household Surgery By Using Weighted Product Method." In *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1-6. IEEE, 2018.

[23]. Taufik, I., A. Saleh, C. Slamet, D. S. Maylawati, M. A. Ramdhani, and B. A. Muhammad. "Decision support system design for determining brown sugar quality with weighted product method." In *Journal of Physics: Conference Series*, vol. 1280, no. 2, p. 022019. IOP Publishing, 2019.

[24]. Divayana, D. G. H., A. Adiarta, and I. B. G. S. Abadi. "Initial draft of CSE-UCLA evaluation model based on weighted product in order to optimize digital library services in computer college in Bali." In *IOP Conference Series: Materials Science and Engineering*, vol. 296, no. 1, p. 012003. IOP Publishing, 2018.

[25]. Bachriwindi, Aniqoh, Erwin Kristian Putra, Umi Madinatul Munawaroh, and A. T. W. Almais. "Implementation of Web-Based Weighted Product Use Decision Support System to Determine the Post-Disaster Damage and Loss." In *Journal of Physics: Conference Series*, vol. 1413, no. 1, p. 012019. IOP Publishing, 2019.