Journal for Educators, Teachers and Trainers
The PROFESIOLab electronic, peer-reviewed, open-access Magazine

ISSN1989–9572

DOI:10.47750/jett.2020.11.01.010

Cloud Data Security: Identifying Challenges and Implementing Solutions

Sukender Reddy Mallreddy[1]

Journal for Educators, Teachers and Trainers,Vol.11(1)

https://jett.labosfor.com/

Date of reception:15 April 2020

Date of revision: 12 July 2020

Date of acceptance:18 September 2020

Sukender Reddy Mallreddy (2020). Cloud Data Security: Identifying Challenges and Implementing Solutions. *Journal for Educators, Teachers and Trainers*, Vol.11 (1).96 -102.

---

[1]Salesforce Consultant, City of Dallas, Dallas, TX USA, Sukender23@gmail.com

Journal for Educators, Teachers and Trainers
The LabOSfor electronic, peer-reviewed, open-access Magazine

Journal for Educators, Teachers and Trainers, Vol.11(1)
ISSN1989– 9572
https://jett.labosfor.com/

Cloud Data Security: Identifying Challenges and Implementing Solutions

Sukender Reddy Mallreddy[1]
[1]Salesforce Consultant, City of Dallas, Dallas, TX USA, Sukender23@gmail.com

ADSTRACT
Cloud data security systems help to protect all the confidential information of any business to develop their organisational goals. The cloud-based model allows the identification of key points which allows analysis of the area of cyber threats for improving the mitigation process. In developing this study researcher are focusing on the impact of the data breaches in the organisation and the effects of the security system after the implication of the technical tools in their organisational performance. All implementation strategies can reduce the impact of data vulnerabilities.

Keywords: Cloud security, data security, cloud computing, cloud computation,

Introduction
Cloud data security is capable of protecting all the stored information and also capable of providing the security system against other motion security threats, theft, corruption and unauthorized access to confidential information. Cloud security systems are designed to protect cloud-based infrastructure, data and applications. This security system also has some challenges which is reducing the effectiveness of this organisational performance by technical implication. This study allows for the identification of all challenges and their mitigating strategies for developing the efficiency of using cloud computing security systems. This study is developed based on the secondary analysis of all types of information of cloud data security systems. All the mitigation strategies of finding challenges help improve the working performance of any organisation to protect their confidential information from leakage. Discussion and conclusion segment allows for evaluating the key findings of this study with the effects of this study in future.

Related work

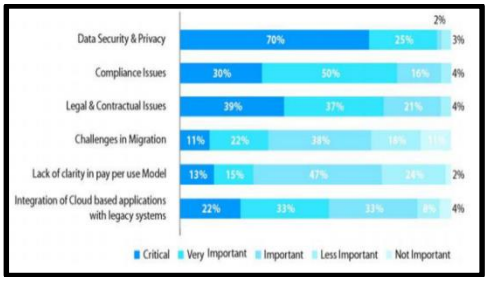

Figure 1: Data security and privacy by cloud-based system
(Source: [1])

Data security and privacy are most important for increasing the effectiveness of organisational performance. Cloud service users are capable of storing all local information in their remote data users [1]. Cloud data security systems are developing their performance with the help of some specific security systems such as data security infrastructure, software services environments such as IaaS, SaaS, and PaaS, and data security platforms. This is effectively mitigating all the issues which are created by human errors, and vulnerable attacks. Different types of multi-cloud data security systems are effective for protecting all the information.

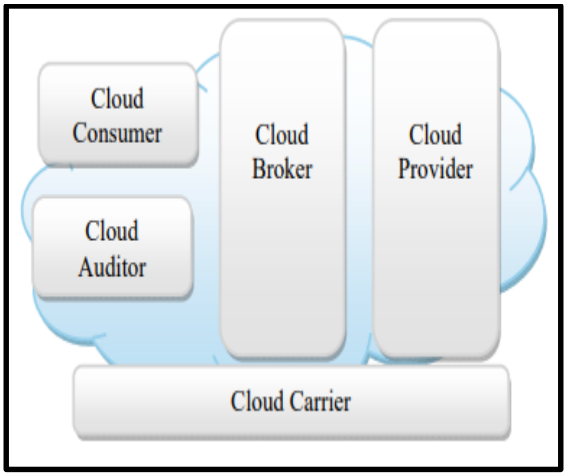

Figure 2: Element of the cloud computation of data protective system
(Source: [2])

Cloud service consumers and cloud service providers all are most effective for increasing delivery models service and data protective systems for all cloud-based information. IaaS helps in developing infrastructure in cloud-based systems such as storage, networks, virtualization, and servers. Based on cloud service consumers the organisation is capable of developing its operations system. All of the elements are linked to each other to provide better strategic planning to develop better data-protecting action to mitigate the effects of cloud data security challenges. Four major types of providing effects of the performance of data security issues ([2]). The four major security issues include; CIA Related Security Issues, issues of Session, Broken Authentication and Controls, Authentication and Access Control, and Data Related Security Issues.

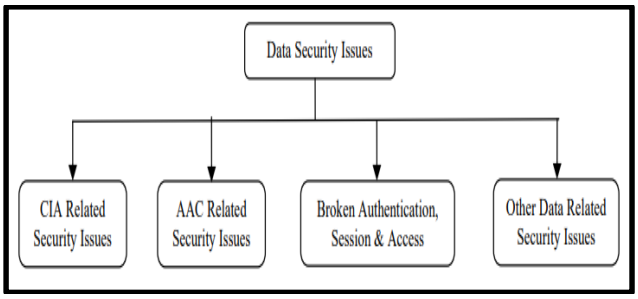

Figure 3: Types of data security issues in cloud bases system
(Source: [2])

The network-based information of cloud data security systems has environmental effects which allow for protection against the unethical leakage of the information. This is the virtual technology with self-service abilities for maintaining computing resources depending on networking infrastructure [3]. Three types of cloud environments are effective for increasing the working performance of the cloud-based data security system such as private, public and hybrid cloud-based technical tools. Generally, the cloud computing data security system is effective for increasing the scalability and flexibility of the computer processing system for reducing the leakage of all confidential information.

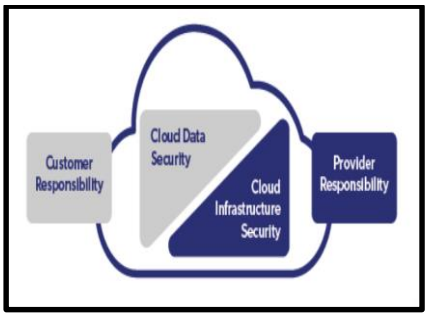

Figure 4: Diagram of cloud data security system
(Source: [4])

The challenges of vulnerabilities happen for hardware, software and firmware for reducing the effectiveness of the cloud working system. According to the report of IDC around 61% of data breaches occur due to the harmful impact of cloud-based technology [4]. The misconfiguration of the information is one of the most vulnerable activities which is data leakage. The poor practices with encryption keys are reducing the effects of the data-controlling system and creating issues in the data security performance. With the help of a better security system by cloud-based data security, an organisation is capable of improving its business goals and developing its marketing capability quickly without any type of failure. This technical implication is also effective in reducing the effects of huge spending of cost.

3. Material and methods

Developing this study research uses secondary data collection methods. All the information is collected from previous research journals, articles, papers and authentic websites. After collecting all the information investigators are analysing those based on secondary analysis for evaluating the outcomes of this study. The collection of the information based on authentic sources helps for mating the authentication of the finding. For improving the cloud data security system investigators need to determine unique security requirements, which is effective for analysing the sources of threats [5]. After evaluating the source of data breaches this organization needs to focus on all the mitigating strategies which is efficient for removing all issues and maintaining user authentication. The combination of LDAP, SSO and PKI helps to address the main threats and location of data leakages. With the bits of help of secondary sources, researchers are capable of analysing all of these efficient ways to determine the key points of data breaches.

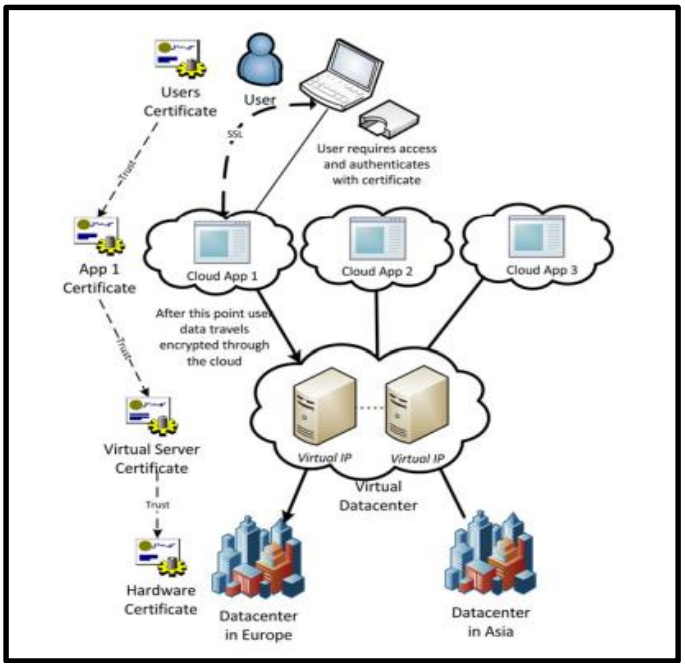

Figure 5: Authentication of User application by cloud service system
(Source: [5])

4. Implementation

Misconfiguration is the biggest threat to cyber security issues in organisational performance. This is mostly responsible for reducing the working procedure in the organisation and responsible for 65% of data leakages. These security issues in cloud computing are playing and major role in the organisational performance of information technology [6]. With the help below image, researchers are capable of evaluating the effects of the security system for increasing organisational performance. This challenge develops after the current adoption of scepticism. The purpose for mitigating all of those issues the organisation need to implement various strategic planning for reducing the bad impact of virtual and economic issues in the cloud computational technologies.

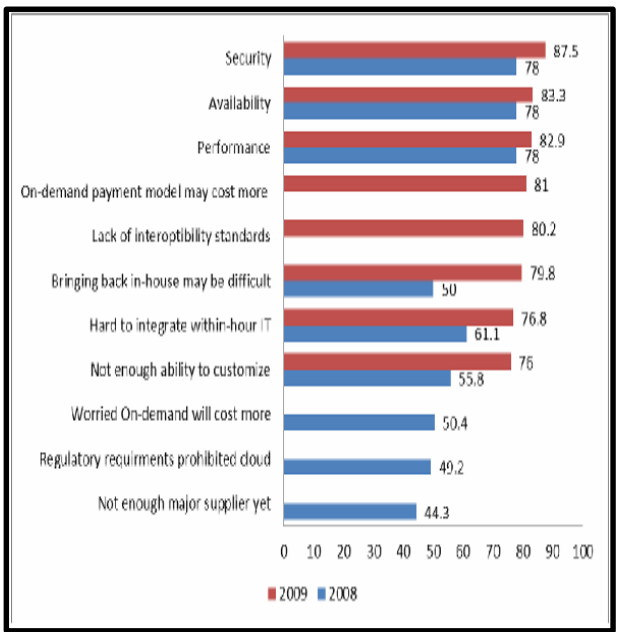

Figure 6: The result of the IDC survey on the effects of cloud security challenges
(Source: [7])

The survey analysis by an international data corporation is conducted the analyse the impact of security services systems after the implementation of cloud-based technology in the organisational working performance. The vulnerability mitigating program is effective for reducing the impact of the cloud data security system [8]. The network classification system is more efficient for prioritizing the mitigating effects for reducing the impact of data leakage. The instalments of configuration networks and instalments of the latest software system help to reduce the impact of data leakage by protecting the data security and privacy management system. By implicating firewalls, increasing bandwidth and antivirus for cloud computation helps prevent all data security risks.

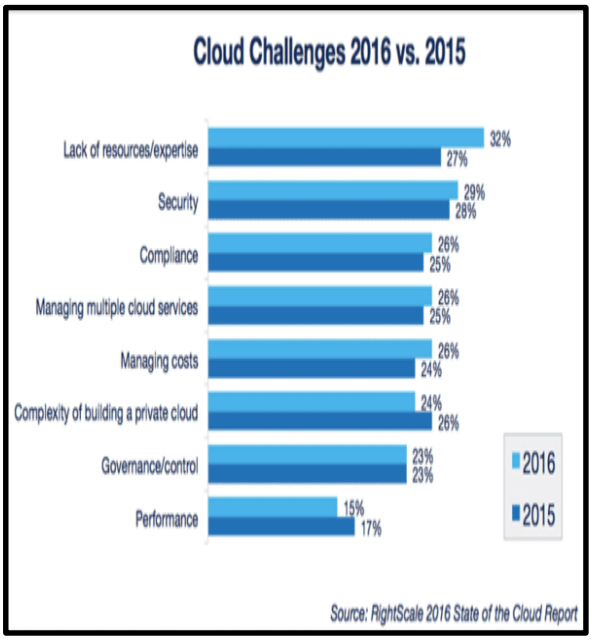

Figure 7: The result of the IDC survey from 2015 to 2016 on the effects of cloud security challenges
(Source: [9])

The above image helps focus on the effects of implementing data security planning to reduce the impact of data breaches and data leakages. Using hacker systems e-learning platforms are capable of determining all the authorized and unauthorized access to the computer to protect all the information from leakage or any type of cyber-attack [10]. The different types of hackers are white hats, grey hats, black hats, script kiddies, blue hats,

neophytes, elite hackers and so on. Among all of these hackers, some help the government to protect their information and some are used for creating a cyber-threat for a government or any organisation.

5. Analysis of Experiment

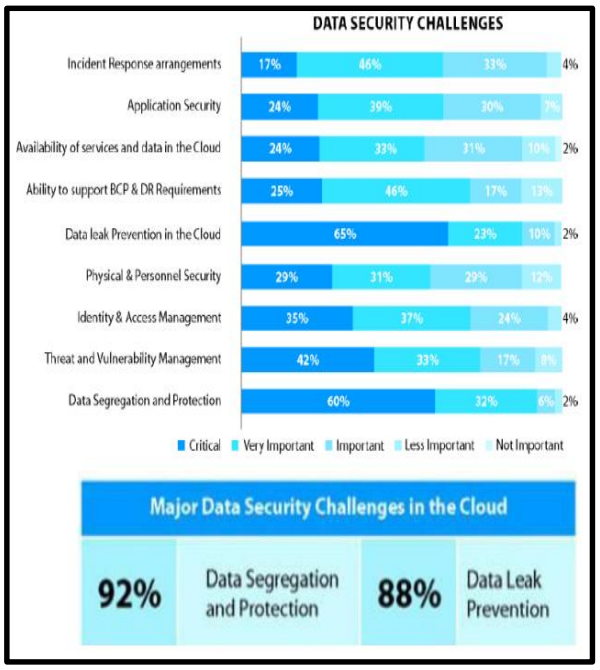

Figure 8: Data Security Challenges
(Source: [1])

Data leakage is providing several impacts on the organisational performance of brand, business and trust areas, which is capable of reducing the effectiveness of the organisational performance. With 88% of important and critical challenges faced by the association for preventing the effects of data leakage. Around 92% of the impact is provided by data segregation and protection for mitigating the effects of security challenges. American IT professionals are developing their cloud computing services compared with the legacy system, which was developed by the survey analysis that was conducted in 2015 by Cluth.co [11]. Around 64% of responders rated the infrastructure of cloud data security planning among all of the organisations.

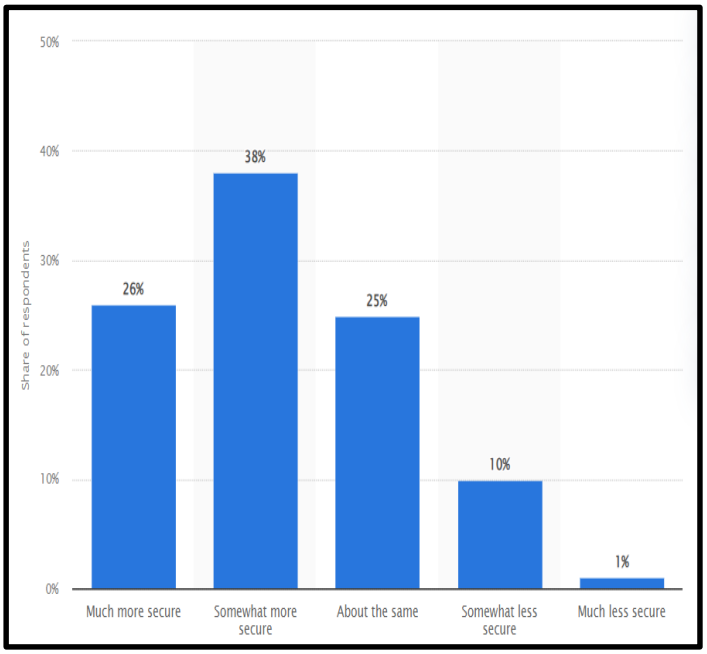

Figure 9: Compared with the legacy system by cloud-based data surety
(Source: [11])

Reducing the effects of multi-cloud environments such as errors of configuration, data governance, lack of security patches and other challenges is the most difficult to track. The purpose for mitigating the effects of the multi-cloud, the need to implicate specific security functionalities, and sophisticated growth of the technical

tools for developing the organizational issues. Using Terraform an organisation is capable of dealing with all the multi-cloud architectures for reducing the impact of data leakage. During the data migration, the handling of data inception is most effective for improving the flexibility and interoperability of confidential information.

6. Discussion

Cloud data security systems are efficient for mating the data security planning of individual organizations to developing growth. This is effective for protecting the information of users to gain their trust and satisfaction. Cloud-based technology implication is effective for saving operational expenditure and protecting capital expenditures for an organisation [12]. By implication of different strategic planning cloud based systems are capable of reducing the impact of data leakage. Technological development helps to increase the marketing valuation and yearly revenue of any organisation and also in e-learning sectors this technical implication is efficient for improving the educational quality and encouragement among children. Moreover, cloud cloud-based data security systems are capable of maintaining all confidential information from any type of technical threat.

The cloud computing paradigm offers for improving the technical implications and the organisational performance of any business sector. Using these technical approaches, the management team is capable of reporting IT investment without an upfront cultural system. The cloud model adoption is efficient for t reducing the issues of their implications by implicating some technical tools and data protection action by vulnerabilities. This is also effective for improving the development of the multi-tendency sharing system among the different service management working procedures for reducing the risk of data leakage during the information transfer.

7. Conclusion and future work

Analysing the overall study, it evaluates that the cloud computing technology is effective for protecting the data security for any type of organisation. The purpose for mitigate all the challenges of this application, the management team needs to implement better data protection and security systems. Mitigating all the challenges for data protecting issues in the cloud computational technologies for reducing the impact of the data breaches and security threats. Based on this study researcher are focusing on the challenges and their implications planning to allow the future researcher to analyse their topic. Evaluating this study reader are capable of increasing their mind set for improving their knowledge regarding cloud data security.

References

[1] Rao, R.V. and Selvamani, K., 2015. Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, pp.204-209.

[2] Kumar, P.R., Raj, P.H. and Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, pp.691-697.

[3] Sabahi, F., 2011, May. Cloud computing security threats and responses. In *2011 IEEE 3rd International Conference on Communication Software and Networks* (pp. 245-249). IEEE.

[4] cpl.thalesgroup.com (2019) *Cloud Data Security Solutions*, *Thales*. Available at: https://cpl.thalesgroup.com/cloud-security (Accessed: 07 June 2024).

[5] Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), pp.583-592.

[6] Kuyoro, S.O., Ibikunle, F. and Awodele, O., 2011. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), pp.247-255.

[7] Babu, L.D., Krishna, P.V., Zayan, A.M. and Panda, V., 2011. An analysis of security related issues in cloud computing. In *Contemporary Computing: 4th International Conference, IC3 2011, Noida, India, August 8-10, 2011. Proceedings 4* (pp. 180-190). Springer Berlin Heidelberg.

[8] Popović, K. and Hocenski, Ž., 2010, May. Cloud computing security issues and challenges. In *The 33rd international convention mipro* (pp. 344-349). IEEE.

[9] Alzhrani, K.M. and Alotaibi, F.S., 2016. Ensuring Security and Privacy for Cloud-based E-Services. *International Journal of Computer Applications*, *149*(11).

[10] Durairaj, M. and Manimaran, A., 2015. A study on security issues in cloud based e-learning. *Indian Journal of Science and Technology*, pp.757-765.

[11] Borgeaud, A. (2016) *Enterprise perceptions of cloud security 2015*, *Statista*. Available at: https://www.statista.com/statistics/541201/united-states-cloud-security-survey-security-perceptions/ (Accessed: 07 June 2024).

[12] Subramanian, N. and Jeyaraj, A., 2018. Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, pp.28-42.