Journal of Coastal Life Medicine
www.jclmm.com
ISSN: 2309-5288(Print)/2309-6152(Online)
Volume 10 No.1 (2022), Page No. 01 – 03
Article History: Received: 02 January 2022, Revised: 10 February 2022, Accepted: 21 February 2022, Publication: 31 March 2022

Healthcare Information System Technique Analysis

Aditya Jayaraman
Department of Biotechnology, Dravidian University, India

Abstract

Healthcare information system methods refer to specific frameworks applied in computer systems to dictate users' accessibility to specific objects. In this case, it is the strategy applied in limiting access to the computers virtual, physical, and system resources. It is also the process by which users gain privileges and are granted access to information, resources, and systems. To facilitate this process and assure access, users must present specific credentials and details that are verified to corroborate the user's identity; thereby ensuring security. For instance, a username and login password can act as a healthcare information system, granting a user access to a secured computer system. However, this option does not guarantee security because the credentials can be transferred to another user. A more secure system could include a thumbprint or retinal scanner that is unique to specific users and, cannot be transferred. In this respect, healthcare information system can be construed as a strategy for securing computers by supporting authorization, authentication, and auditing processes that identify the user seeking access to the system. As such, healthcare information system is a practice responsible for securing information and setting privileges towards the identification of a specific user, listing sites that can be accessed, and the time when access is allowed. Notably, the entire security system is offered by administrators. This study proposed a hybrid healthcare information system technique to discern its efficiency, as well as future implications for the field of healthcare systems.

1 Introduction

Healthcare information system entails providing permission, as well as a group of users to whom the permission applies. Indeed, three principal methods of healthcare information system are available; differentiated by the level of security provided, as well as the nature of protocols governing the users' right to use. The three methods include discretionary healthcare information system (DAC), mandatory healthcare information system (MAC), and role-based healthcare information system (RBAC). DAC involves healthcare information systems that are coordinated by the owner of the file or site, and that the owner selects authorized individuals to access the file – using control lists. Therefore, DAC is used in small business arenas. On the other hand, MAC involves the application of greater structures that classify users before categorizing levels regarding the amount of access that is allowed. In essence, it is based on both the clearance level of the user and data, as well as the object's classification. Organizations that commonly use this method include CIA, FBI, all the branches of the US Military, and Federal Agencies. In contrast to DAC, MAC coordinates access through the rules configured by administrators. Lastly, RBAC presents a set of controls that govern access to data on the basis of roles, rather than user specificity. Specifically, RBAC decides the amount of information the receptionist can access while ensuring that the site's manager has greater access than the receptionist groups (Vacca, 2013). Indeed, RBAC works better in companies that experience high turnover.

2 Methodology

The three principal methods of healthcare information system pose mixed outcomes that comprise advantages and disadvantages. This variation makes the approaches appropriate in different and specific scenarios (or situations). DAC has the advantage of offering and enforcing a good security policy. This merit is informed by the fact that the file's owner exhibits the capacity to grant or deny access to the system; fostering absolute control. However, the approach is disadvantageous in such a way that it applies to single or small systems and companies – because it does not differentiate levels of security clearance; making it difficult to apply in larger firms.

3 Results and Discussion

It is evident that negative aspects of healthcare information system methods revolve around the amount of security provided and thenumber of security levels it can support. This affirmation implies that specific healthcare information system methods ought to be matched with specific scenarios to mitigate risks. In this case, DAC is only appropriate for small organizations with few employees and a single level of users. This arrangement ensures that its disadvantages, which are exposed upon being applied in large companies with multiple layers of users,are mitigated. Furthermore, RBAC is appropriate for both small and large organizations with single and multiple levels of users, making it inappropriate for organizations whose users perform multiple roles. The implication is that the best strategy for mitigating negative aspects arising from the methods of healthcare information system is to apply them to specific organizations in which they are better suited (Bhardwaj, 2007; Vacca, 2013).

The present case is concerned with the provision of information security for a medium-sized federal government contractor. The organization has many task forces and user groups who require multiple levels of access. As such, there is a need for adequate security because of the fact that it is a government contractor whose role involves handling state-related affairs. Given the state of the firm, it becomes appropriate to select an healthcare information system method that will allow for multiple levels of access, useful in large organizations while offering a desirable level of system security.

Whereas findings suggest that MAC is the best option, weaknesses remain inevitable. The first challenge involves the development of an effective system that could be applied on a firm-specific basis; as the process of satisfying both the stakeholders' needs and user preferences is likely to pose a dilemma. This challenge could be mitigated by identifying specific levels of the security system and clearance, as well as the projected number of people that will access the information − from respective access points. Also, the challenge can be mitigated by evaluating the available MACs in the market and selecting those that match the needs of the company. The second challenge concerns the process of hiring task forces in the IT division. The challenge is specifically attributed to the need for expertise in the practices of setting up and managing the MAC system, as well as correcting links when the need arises. This challenge can be mitigated by employing qualified and experienced IT personnel. The final challenge concerns the need to ensure that the company's personnel have the capacity to use the selected MAC appropriately. Despite its complexity, the challenge can be mitigated by holding seminars and conferences to embrace employee training and development or functional path provision towards better performance (Lehtinen, Russell &Gangemi, 2006; Solomon, 2013).

Article History: Received: 02 January 2022, Revised: 10 February 2022, Accepted: 21 February 2022, Publication: 31 March 2022

4 Conclusion

In conclusion, it is evident that system security is an important concept in information management. Specific concern arises in situations where the data management system involves computers. In this study, outcomes suggest that the healthcare information system methods serve to address sections of security concerns by securing data in both the authorized and restricted states. Specific healthcare information system methods that have been examined include DAC, RBAC, and MAC. Whereas the three options are critical to data security operations, MAC has been selected as the most appropriate system for the selected company. The documentation is informed by the capacity of MAC's merits to surpass potential disadvantages. In summary, it can be inferred that healthcare information system is an approach responsible for securing information with the intention of identifying and authorizing specific site user groups. By adopting MAC as an appropriate healthcare information system technique, it is projected that the company will realize an improved level of performance − in terms of user access to the system, as well as data security.

References

[1]. Bhardwaj, P. K. (2007). *A+, Network+, Security+ Exams in a Nutshell: A Desktop Quick Reference*. Sebastopol, CA: O'Reilly Media, Inc.

[2]. Lehtinen, R., Russell, D. &Gangemi, R. (2006).*Computer Security Basics, (2nd Ed.).* Sebastopol, CA: O'Reilly Media, Inc.

[3]. Solomon, M. G. (2013). *Security Strategies in Windows Platforms and Applications, (2nd Ed.).* Burlington, MA: Jones & Bartlett Learning

[4]. Vacca, J. R. (2013). *Computer and Information Security Handbook, (2nd Ed.).* Waltham, MA: Morgan Kaufman Publishers