WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security and Privacy Challenges Hindering the Adoption of E-Healthcare Systems

Mageto Stephen N[1], Patrick Kipkorir Laboso [2]

[1]Department of Computer Science, Karpagam Academy of Higher Education (KAHE), Coimbatore, 641021, India. magetosteve@gmail.com
[2] Department of Computer Science, Central University of Tami Nadu, Thiruvarur, 610005, India. Labosopatrick95@gmail.com
DOI: https://doi.org/10.55248/gengpi.4.1223.0116

ABSTRACT:

The adoption of e-healthcare systems is significantly hindered by privacy and security concerns, as exposure and abuse of personal health information can lead to serious privacy breaches for patients. Patients may suffer from unequal treatment, such as termination of employment or insurance if their deteriorating health condition becomes known to their employers. Despite the general assumption that the cloud operates under the honest-but-curious model and can execute protocol specifications perfectly, it is still vulnerable to extracting a patient's private PHI during data transmission and storage. This paper highlights the potential risks associated with such systems, including the possibility of inequitable treatment, termination of contracts, and insurance policies. The paper also discusses the use of cloud-based systems and the challenges they present in terms of security management and scalability. It concludes by stressing the importance of addressing these issues to develop a more robust e-healthcare system.

Keywords: e-healthcare, security, privacy, personal health information, cloud, scalability.

1. Introduction:

E-healthcare systems have the potential to revolutionize the delivery of healthcare services by improving patient outcomes, reducing costs, easy access to medical information and remote consultations [7]. However, privacy and security concerns have hampered the wide adoption of such systems. The exposure and abuse of personal health information (PHI) can lead to serious privacy leaks for patients. In addition to the impact on the patient's health, the disclosure of PHI can also result in inequitable treatment, such as the termination of labor contracts and insurance coverage. Therefore, it is crucial to address security and privacy issues to enable wider adoption of e-healthcare systems. This paper focuses on the privacy and security issues associated with e-healthcare systems and the challenges of implementing cloud-based systems.

2. Discussion:

One of the primary concerns with e-healthcare systems is the potential for PHI exposure during data transmission and storage [5]. The cloud is often used to store medical information and facilitate data transmission, but it is generally assumed to operate under the honest-but-curious model. This means that while the cloud provider may not intentionally compromise the privacy of patient information, they may still have access to it and be able to extract it during transmission or storage.

To mitigate the risks of PHI exposure, security management and scalability must be addressed. Security management involves implementing appropriate measures to protect PHI from unauthorized access or disclosure [6]. This may include encryption, access control, and regular security audits. Scalability refers to the ability of the system to handle large amounts of data and users without compromising security or performance. This is particularly important for e-healthcare systems, which must be able to handle a large volume of patient data and user requests.

3. Security and Privacy Challenges in e-Healthcare Systems

Privacy Concerns: The exposure and abuse of personal health information (PHI) is a major concern in e-healthcare systems [1]. The release of such information can result in serious privacy breaches for patients, which can have long-lasting consequences. Patients are likely to suffer from not only the disease but also the inequitable treatment, such as termination of labor contracts and insurance policies. In addition, the transfer and storage of PHI in the cloud environment present significant risks of unauthorized access and data breaches [10].

3.1 Security Concerns

Security issues are also a major concern in e-healthcare systems. Hackers and other malicious actors can target such systems to gain access to PHI, which can be sold on the black market or used for identity theft [4]. The use of cloud-based systems can exacerbate this problem, as these systems are generally assumed to be under the honest-but-curious model. This means that while the cloud provider may not intentionally disclose PHI, it may still extract such information during the transmission of data or while storing the data.

3.2 Cloud-based Systems

Cloud-based systems have become increasingly popular in e-healthcare systems due to their scalability and cost-effectiveness [8]. However, the use of such systems presents significant challenges in terms of security management and scalability. Cloud-based systems are generally less secure than on-premise systems and require extensive security measures to ensure that PHI is not compromised [9]. In addition, these systems may not be able to scale effectively to meet the growing demand for e-healthcare services.

4. Practical Difficulties in Creating a Better e-Healthcare System

To create a better e-healthcare system, practical difficulties such as security management and scalability must be addressed.

4.1 Security management

This involves implementing robust security measures to protect PHI from unauthorized access and disclosure. This includes implementing access controls, encryption, and firewalls to prevent data breaches and cyber-attacks [2]. Additionally, healthcare organizations must develop policies and procedures for securely transmitting and storing PHI in the cloud.

4.2 Scalability

Scalability is another practical difficulty that needs to be addressed in creating a better e-healthcare system. As the volume of PHI grows, the system must be able to handle the increased demand without compromising security and privacy [3]. This requires the implementation of scalable and flexible infrastructure that can accommodate the growing demands of e-healthcare systems.

5. Conclusion

The adoption of e-healthcare systems has revolutionized the healthcare industry, making it more accessible, efficient, and affordable for patients. The development of a robust e-healthcare system requires the effective management of privacy and security risks. While cloud-based systems offer significant benefits in terms of scalability and cost-effectiveness, they also present significant challenges in terms of security management, scalability, potential exposure and abuse of PHI which can result in serious privacy breaches for patients. To overcome these challenges and create a better e-healthcare system, e-healthcare providers must invest in robust security measures and ensure that PHI is protected at all times. Only by addressing these issues can we develop a truly effective and safe e-healthcare system.

Reference

1. 1.Yang, X., Lu, R., Shao, J., Tang, X., & Yang, H. (2018). An efficient and privacy-preserving disease risk prediction scheme for e-healthcare. *IEEE Internet of Things Journal*, *6*(2), 3284-3297.
2. Kute, S. S., Tyagi, A. K., & Aswathy, S. U. (2022). Security, privacy and trust issues in internet of things and machine learning based e-healthcare. *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, 291-317.
3. Ishak, M., Rahman, R., & Mahmud, T. (2021, November). Integrating Cloud Computing in E-healthcare: System Design, Implementation and Significance in Context of Developing Countries. In *2021 5th International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)* (pp. 1-6). IEEE.
4. Kumar, A., Bhushan, B., Shristi, S., Kalita, S., Chaganti, R., & Obaid, A. J. (2023). Blockchain embedded security and privacy preserving in healthcare systems. In *Blockchain Technology Solutions for the Security of Iot-Based Healthcare Systems* (pp. 241-261). Academic Press.
5. Rhoads, J. (2023). Identifying Ethical and Legal Issues in the Use of Patient Health Information for Research and Quality Improvement. *International Journal of Intelligent Automation and Computing*, *6*(1), 17-30.
6. Puder, A., Henle, J., & Sax, E. (2023, March). Threat Assessment and Risk Analysis (TARA) for Interoperable Medical Devices in the Operating Room Inspired by the Automotive Industry. In *Healthcare* (Vol. 11, No. 6, p. 872). MDPI.
7. Gupta, B. B., Gaurav, A., & Panigrahi, P. K. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, *162*, 113859.

8. Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital Transformation in Healthcare: Technology Acceptance and Its Applications. *International Journal of Environmental Research and Public Health*, *20*(4), 3407.

9. Krumm, N. (2023). Organizational and Technical Security Considerations for Laboratory Cloud Computing. *The Journal of Applied Laboratory Medicine*, *8*(1), 180-193.

10. Livanis, E., Doumpos, M., & Zopounidis, C. (2023). Financial analysis and management of cyber risk. In *Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship* (pp. 255-271). Edward Elgar Publishing.