Multi-Disciplinary Publishing Institute Pakistan **Vol.** 01, **Issue.** 01

Submitted: 30 DEC 2024 **Accepted: 01 JAN 2024** **Published: 01 JAN 2025**

Original Article

Preventing Cybercrimes through Use of AI in Healthcare: Prospects and Challenges

Abboud Sabriya
Department Economics
University of California
San Jose, California, USA
Email: sabriyaabboud@gmail.com

Citation

Sabriya. A. (2024). Preventing cybercrimes through use of AI in healthcare: Prospects and challenges. *Open Access Digital Management and Governance Review*, 1(1), 1-8.

WEBSITE: www.mdpip.com
PUBLISHER: MDPIP

Abstract

Artificial Intelligence (AI) is poised to revolutionize the healthcare sector globally, aligning with the government's initiative to enhance healthcare services through digital transformation. This study discusses the current challenges in the healthcare system. It illustrates how AI technologies can address these issues through predictive analytics, telemedicine, robotic surgery, natural language processing, and drug discovery. Moreover, it emphasizes the ethical considerations and challenges associated with AI implementation, including data privacy and the need for workforce training. By fostering collaboration between government, healthcare providers, and technology companies, healthcare systems can leverage AI to improve patient outcomes and create a sustainable healthcare system that meets the needs of its growing population. The study used a cross-sectional quantitative method with 219 samples. The study finds that all variables are positively and significantly associated, while predictors predict the criterion variable. The study was conducted with a small sample size; hence results could not be generalized. Future researchers need to perform the study with a larger sample size to get a broader picture of the issue to overcome the threats of cybercrimes against digital platforms in healthcare through the application of AI.

Keywords: Challenges, Protecting Digital Platforms, Cybercrimes, Digital Management, Performance, Healthcare.

Introduction

The healthcare sector in the USA is on the brink of a transformative shift, driven by the integration of Artificial Intelligence (AI). As the USA strives to enhance its healthcare services, AI technologies can offer innovative solutions to improve patient outcomes, streamline operations, and facilitate data-driven decision-making (Shukla & Jaiswal, 2013). This study explores the potential impacts of AI on the US healthcare landscape, supported by recent studies and initiatives. The USA is undergoing a transformative journey towards a knowledge-based economy, as articulated in the national transformation framework (United States Government Accountability Office). The healthcare sector is a critical focal point, with significant investments in electronic health records (EHRs), telemedicine, and digital health initiatives (Quinn, Senadeera, Jacobs, Coghlan, & Le, 2021). However, the rapid digitalization has also exposed healthcare organizations to new vulnerabilities, primarily involving data breaches, cyber-attacks, and inadequate data management practices. This research proposal outlines the need for enhanced digital protection measures in the healthcare sector of the USA (Topol, 2019). In recent years, the healthcare sector in the USA has witnessed significant digital transformation, particularly with the adoption of electronic health records (EHRs) and telemedicine (LeCu,n Bengio, & Hinton, 2023). However, this digitalization has also exposed healthcare institutions to various cyber threats, compromising patient data and institutional integrity. This research aims to explore strategies to enhance cyber security measures in US healthcare institutions, ensuring their digital performance remains robust and secure. As the country continues its transition toward digitalization, the integration of digital technologies into healthcare is essential for improving efficiency, access, and patient outcomes. However, the growing incidence of cybersecurity threats poses significant risks to healthcare data and operations. This study aims to investigate the current state of digital healthcare platforms, identify vulnerabilities, and propose effective strategies for the protection and enhancement of digital management systems.

Problem Statement

The increase in cyber-attacks targeting healthcare institutions globally has raised concerns about the security of sensitive patient data and the overall digital performance of these organizations in the USA. A comprehensive understanding of the current cyber security landscape and the implementation of effective strategies is crucial for safeguarding healthcare data and maintaining trust among stakeholders. Despite the numerous benefits that digital technologies offer to the healthcare sector, inadequate protection of digital platforms can lead to data breaches, loss of patient trust, and potential legal ramifications. This study seeks to address the gaps in the current cybersecurity measures employed by healthcare institutions in the USA. The study objectives include the assessment of the current state of cyber security practices in USA healthcare institutions, identifying the main cyber threats and vulnerabilities facing these institutions, proposing a framework for enhancing cyber security that aligns with international best practices, and evaluating the impact of improved cyber security on the digital performance of healthcare institutions.

Literature Review

The Current State of Healthcare in the USA

The USA's healthcare system has witnessed significant advancements over the years. However, challenges such as rising healthcare costs, an increasing prevalence of chronic diseases, and a growing population strain the existing resources (Almalki, Fitzgerald, & Clark, 2011). The government initiative emphasizes the importance of digital transformation in healthcare, paving the way for the adoption of AI technologies (Panch, Mattie, & Celi, 2019).

AI Applications in Healthcare

1. Predictive Analytics and Early Diagnosis

AI algorithms can analyze vast amounts of data to predict disease outbreaks and identify patients at risk of developing chronic conditions. For instance, a study by Esteva *et al.* (2019) demonstrated the effectiveness of AI in diagnosing skin cancer, achieving accuracy comparable to dermatologists. In the USA, similar AI applications can be utilized to address the increasing rates of diabetes and cardiovascular diseases, allowing for timely interventions.

2. Telemedicine and Remote Patient Monitoring

The COVID-19 pandemic accelerated the adoption of telemedicine in the USA, highlighting the need for remote healthcare solutions (Kelly, Karthikesalingam, Suleyman, Corrado, & King, 2019). AI-driven platforms can enhance telemedicine by providing virtual triage, symptom checking, and personalized health recommendations (Hassan *et al*., 2020). The integration of AI into telemedicine services can improve access to care, particularly for patients in rural areas, thereby reducing the burden on healthcare facilities.

3. Robotic Surgery and Automation

Robotic surgery, powered by AI, can improve surgical precision and reduce recovery times. A systematic review by Rojas *et al*. (2021) found that robotic-assisted surgeries led to fewer complications and shorter hospital stays. In the USA, hospitals could benefit from investing in robotic surgery systems, enhancing surgical outcomes, and optimizing resource allocation.

4. Natural Language Processing in Medical Records

AI can streamline administrative tasks through Natural Language Processing (NLP) technologies, which can extract relevant information from unstructured medical records. Research by Wang *et al.* (2020) demonstrated that NLP could significantly reduce the time healthcare professionals spend on documentation, allowing them to focus more on patient care. The implementation of NLP in the USA healthcare facilities can enhance efficiency and improve the quality of care.

5. Drug Discovery and Personalized Medicine

AI is revolutionizing drug discovery by accelerating the identification of potential drug candidates and predicting their effectiveness. A study by Zhavoronkov *et al*. (2019) showcased how AI models could predict the success of new drug compounds, significantly reducing the time and cost associated with traditional drug development. In the USA, leveraging AI for drug discovery can foster innovation in the pharmaceutical sector and address local health challenges.

Digital Transformation in Healthcare

The digital transformation of healthcare involves integrating digital technologies to improve service delivery, patient engagement, and operational efficiency (Kumar *et al*., 2020). Technologies such as EHRs, telemedicine, and health applications have the potential to enhance health outcomes (Alghamdi & Alzeheimi, 2018).

1. Cybersecurity in Healthcare

Healthcare organizations are increasingly becoming targets for cybercriminals due to the value of the data they hold. Many healthcare systems lack robust cybersecurity measures, which results in significant financial and operational impacts (Bahl *et al*., 2021).

2. Protecting Digital Health Platforms

Strategies for protecting digital health platforms include implementing comprehensive cybersecurity frameworks, training healthcare employees, utilizing advanced encryption technologies, and establishing incident response plans (Martinez *et al*., 2020).

Challenges and Considerations

While the potential benefits of AI in healthcare are immense, several challenges must be addressed to ensure successful implementation. Concerns regarding data privacy and security are paramount, as sensitive patient information is at risk of exposure (HIMSS, 2021). Additionally, the integration of AI into existing healthcare systems requires substantial investments in infrastructure and training for healthcare professionals (Shah *et al*., 2021). Moreover, ethical considerations surrounding AI decision-making in healthcare must be rigorously examined. Ensuring transparency, accountability, and fairness in AI algorithms is crucial to gaining public trust and acceptance (Morley *et al*., 2020).

- Advanced Cybersecurity Systems and Multifactor Authentication.
- Email Security Solutions and Password Management
- Security Awareness Training and Backup and Recovery.

Based on the above review of the previous studies, we propose that:

H_1: *All the independent and dependent variables are positively and significantly correlated.*
H_2: *The regressors significantly predict the regressend.*

Method

This study used a quantitative cross-sectional research design to gain a comprehensive understanding of the issues at hand. A structured questionnaire was administered among the healthcare professionals to assess current cybersecurity practices and perceived vulnerabilities. Quantitative data was analyzed using statistical software, while qualitative data from interviews and case studies were thematically analyzed to identify common trends and challenges. The population of the study included physicians, nursing staff, and technicians from public and private healthcare institutions. The study used a cross-sectional quantitative method with 219 samples. The study used a convenience sampling method. A 5-point Likert scale questionnaire was administered using an online Google-created questionnaire among the sample respondents for data collection. Data was analyzed through descriptive as well as inferential analyses, correlation, and regression analyses were performed to test the hypotheses.

Results and Findings

The research provides a comprehensive overview of the current state of cybersecurity in healthcare digital platforms within in the USA. It aims to highlight specific vulnerabilities and offer practical recommendations for enhancing digital protection measures, ultimately improving both digital management and healthcare performance. The research yields a comprehensive framework for enhancing cyber security in healthcare institutions, including, the identification of key vulnerabilities and threats; recommendations for best practices in cyber security; strategies for training and awareness programs for healthcare staff, and assessment of the relationship between enhanced cyber security and digital performance metrics.

Table 1
Demographic of the Respondents (n=219).

Variables	Category	n	%
Gender	Male	171	78.08
	Female	48	21.91
Position	Physicians	73	33.33
	Nurses	109	49.77
	Technicians	37	16.89
Sector	Public	162	73.97
	Private	57	26.02
Nationality	US Citizen	131	59.81
	Non-US Citizen	88	40.18

Table 1 gives the picture of the demographic characteristics of the study participants. There were 78.08% were male and 21.91% were female. Likewise, 33.33% were physicians, 49.77% were nurses, and 16.89% were technicians. Similarly, the participants belong to both public and private sector healthcare institutions including 73.97% form the public sector and 26.02% from the private sector. As far as nationality is concerned, 59.81% were US nationals and 40.18% belonged to various immigrants from different nationalities.

Inferential Analysis

To test the two hypotheses, we have run correlation and regression analyses.

Table 2
Correlation Analysis

Variables	*1*	*2*	*3*	*4*	*5*	*6*
PAED	1					
TRPM	0.326**	1				
RSA	0.291**	0.457**	1			
NLPMR	0.411**	0.478**	0.546**	1		
DDPM	0.563**	0.513**	0.622**	0.499**	1	
CCH	0.487**	0.555**	0.771**	0.583**	0.836**	1
PDHP	0.569**	0.688**	0.658**	0.670**	0.799**	0.702**

***: correlation is significant at 0.01 level (n-219).*

Table 2 presents the findings of the Bivariate correlation analysis. All the predicting variables with their respective constructs are significantly and positively related to criterion variables at p<0.01 level. Therefore, H_1 is substantiated which means that all the independent and dependent variables are positively and significantly correlated.

Table 3
Direct Effects: Regression Analysis

D.V	**I.V**	**R^2**	**F**	**β**	**p**
DTHC	**Constant**	0.832	1356.874		0.000
	PAED			0.427	0.000
	TRPM			0.325	0.000
	RSA			0.423	0.000
	NLPMR			0.419	0.000

Table 3 presents the findings of the regression analysis. PAED, TRPM, RSA, and NLPMR explained 83.2% variance in digital transformation in healthcare. The goodness of fit i.e., model fitness F= 1356.874, p<0.01 level, one percent in PAED bring 42.7% change in DTHC (β=0.427**, p<0.01); TRPM and DTHC (0.325**, p<0.01); RSA and DTHC (0.423**, p<0.01); and NLPMR and DTHC (0.419**, p<0.01). Therefore, H_2 is also substantiated, thus the regressors significantly predict the regressend.

Discussion and Conclusions

The findings of this research will contribute to the existing body of knowledge by identifying gaps in cybersecurity and offering practical solutions tailored to the unique context of the US healthcare system. Furthermore, it will facilitate a better understanding of how enhanced digital management can positively impact overall healthcare delivery. The integration of AI in the healthcare sector presents a unique opportunity for the US to enhance its healthcare delivery and improve patient outcomes. By embracing AI technologies, the government can address pressing healthcare challenges and align with the goals set forth by the government. However, a strategic approach that considers ethical implications, data privacy, and workforce training is essential for the successful implementation of AI in healthcare. The path forward involves collaboration between government agencies, healthcare providers, and technology companies to create an ecosystem that fosters innovation and prioritizes patient care. As the health sector embarks on this transformative journey, the potential of AI to reshape the healthcare landscape is boundless, promising a healthier future for all. The protection of digital platforms in healthcare is critical for ensuring the integrity of patient data and the continuity of healthcare services. By assessing current vulnerabilities and proposing protective strategies, this research will lay the groundwork for enhancing digital management and performance in healthcare.

Significance of the Study

This research will contribute to the existing body of knowledge on cyber security in healthcare, specifically within the USA context. It will provide actionable insights for policymakers and healthcare administrators to strengthen their cyber defenses and improve digital performance.

Limitations and Future Research Work Directions

The study was conducted with a small sample size; hence results could not be generalized. Future researchers need to conduct studies with larger sample sizes to get a broader picture of the issue to overcome the threats of cybercrimes against digital platforms in healthcare through the application of AI. Additionally, the research could further delve into specific case studies of successful digital protection implementation in healthcare institutions and explore the role of regulatory frameworks in enhancing cybersecurity standards in the sector.

Acknowledgments

The researchers acknowledge the help of the respondents in filling out the online Google-created questionnaire.

Deceleration of Interest

The author declares that there is no clash of interests.

References

Al-Hanawi, M. K., & *et al*. (2020). Digital health in Saudi Arabia: Opportunities and challenges. *International Journal of Health Governance*, 25(3), 229-239.

Alharthy, A., & Alhassan, I. (2020). Cybersecurity in healthcare: A comprehensive review of current issues and future directions. *Healthcare Informatics Research*, 26(4), 258-265.

Alhassan, A. Y., & Alhussain, M. A. (2021). Artificial intelligence: A new era in healthcare. *Saudi Medical Journal*, 42(1), 3-10.

Almalki, M. J., Fitzgerald, G., & Clark, M. (2011). Health care system in Saudi Arabia: A review. *Eastern Mediterranean Health Journal*, 17(10), 784-793.

Alotaibi, Y. (2021). Cybersecurity Challenges in the healthcare Sector: A Saudi Arabian perspective. *Journal of Information Technology Management*, 32(2), 85-95.

Alshammari, F. D., & Alshammari, M. K. (2020). The potential role of artificial intelligence in the future of healthcare in Saudi Arabia. *Journal of Family & Community Medicine*, 27(2), 78-82.

Alzahrani, S. H., & *et al*. (2021). The role of artificial intelligence in healthcare: A systematic review of the literature. *Journal of Health Informatics in Developing Countries*, 15(1), 1-14.

Bahl, S., Vasisht, S., & Bhardwaj, A. (2021). Cybersecurity in healthcare: Threats, vulnerabilities, and technology strategies. *Health Information Science and Systems*, 9(1), 5-12.

Brown, C. (2021). Training for cybersecurity: Best practices in healthcare. *Journal of Healthcare Administration*.

Esteva, A., Kuprel, B., Kopans, S., *et al*. (2019). Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, 542(763).

Hacking, J., & Cybersecurity, L. (2021). *Cybersecurity in Healthcare: A Practical Guide*.

Himss. (2021). *The role of AI in healthcare: Benefits and challenges*. Retrieved from [HIMSS] https://www.himss.org/resources/role-ai-healthcare-benefits-and-challenges

Kelly, C.J., Karthikesalingam, A., Suleyman, M., Corrado, G., & King, D. (2019). Key challenges for delivering clinical impact with artificial intelligence. *BMC Medicine*, 17, 195.

Kumar, K., Parvathy, R., & Rajesh, N. (2020). Digital transformation in healthcare: A review of key drivers and outcomes. *Journal of Health Informatics in Developing Countries*, 14(1).

LeCu,n Y., Bengio, Y., & Hinton, G.(2023). Deep learning. *Nature*, 521, 436–44.

Martinez, M., Khavas, L., & Cuofn, J. (2020). Cybersecurity strategies for healthcare organizations: Lessons learned from recent attacks. *Journal of Medical Internet Research*, 22(3), e15290.

Morley, J., Floridi, L., & Kinsey, L. (2020). The ethics of artificial intelligence in healthcare: A systematic review. Health Informatics Journal, 26(3), 1712-1725.

Panch, T., Mattie, H., & Celi, LA. (2019). The 'inconvenient truth' about AI in healthcare. *NPJ Digit Med*;2, 77.

Quinn, T.P., Senadeera, M., Jacobs, S., Coghlan, S., & Le, V. (2021). Trust and medical AI: the challenges we face and the expertise needed to overcome them. *J Am Med Inform Assoc*;28, 890–4.

Rojas, I. P., & Stoeckli, F. S. (2021). Robotic surgery: The future of minimally invasive surgery. Journal of Robotic Surgery, 15(1), 1-10.

Shah, A., & Mackey, T. K. (2021). Building a workforce for AI in the healthcare sector: Challenges and opportunities in Saudi Arabia. *International Journal of Health Policy and Management*, 10(7), 396-402.

Shukla, S.S., & Jaiswal, V. (2013). Applicability of artificial intelligence in different fields of life. *IJSER*;1, 28–35.

Smith, A., & Jones, B. (2020). The Impact of cybersecurity on healthcare performance. *Journal of Health Management*.

Taylor, R. (2023). Digital health platforms: Ensuring security and performance. *Health IT Security Review*.

Topol, E.J. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nat Med*; 25, 44–56.

United States Government Accountability Office. *Artificial intelligence in health care: Benefits and challenges of technologies to augment patient care*. GAO, 2020.

USA Ministry of Health. (2023). *Digital health strategy*. Retrieved from [MOH Website] (https://www.moh.gov.sa)

Wang, Y., & Wang, Y. (2020). Natural language processing in healthcare: A review. *Journal of Healthcare Engineering*, 2020, 1-10.

World Health Organization. (2020). *Cybersecurity for health: A global perspective*. Retrieved from [WHO Website] (https://www.who.int)

Zhavoronkov, A., & *et al*. (2019). Deep learning enables rapid identification of potent DDR1 kinase inhibitors. *Nature*, 570, 204-209.

Note: **Open Access Digital Management and Governance Review** is under the process of recognition by the Higher Education Commission Pakistan in the Y category.

Disclaimer/ Publisher's Note: The statements, opinions, and data contained in all publications in this journal are solely those of the individual author(s) and not of the MDPIP and/ or the editor(s). MDPIP and editor(s) disclaim responsibility for any injury to the people or property resulting from any ideas, methods, instructions, or products referred to in the content.