Margaret Afwande, 2024, 12:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology

An Open Access Journal

Evaluating the Effectiveness of Blockchain Technology in Mitigating Cybersecurity Crimes in Electronic Health Management Systems within Public Hospitals in Kenya

Margaret Afwande[1], Samuel Barasa[2], Jane Kabo[3]
Department of Information Technology, Kibabii University/Bungoma, Kenya[1,2]
School of Nursing, Kibabii University/Bungoma, Kenya[3]

Abstract- The digital transformation of healthcare fundamentally enhanced the management and accessibility of patient data through the implementation of Electronic Health Management Systems (EHMS). In Kenya, public hospitals increasingly integrated EHMS to optimize healthcare service delivery and improve patient care outcomes. However, this transition introduced significant cybersecurity vulnerabilities, including data breaches and unauthorized access, jeopardizing the confidentiality and integrity of sensitive patient information. This study evaluated the effectiveness of blockchain technology in mitigating these cybersecurity threats within EHMS in public hospitals in Kenya. The research identified that 78% of IT specialists reported data breaches as the most prevalent cyber threat and 64% cited frequent incidents of unauthorized access. Furthermore, 82% of respondents indicated that existing cybersecurity strategies were insufficient to address emerging threats. Despite the recognized limitations of current security measures, 87% of experts expressed confidence in blockchain's ability to enhance EHMS security. The decentralized and immutable nature of blockchain was perceived to significantly mitigate unauthorized access and data tampering, with 90% of respondents agreeing that it could reduce the risks of data manipulation. The qualitative interviews with healthcare professionals revealed concerns about privacy violations and mistrust in the current EHMS. The findings underscored the urgent need for innovative cybersecurity measures, with blockchain emerging as a promising solution. This study contributed valuable insights into the potential advantages and limitations of blockchain technology, establishing a framework for enhancing the security of EHMS in Kenya and informing the development of more secure healthcare information systems.

Keywords- Blockchain Technology, Cybersecurity in Healthcare, Electronic Health Management Systems (EHMS), Data Security, Public Health Informatics

I. INTRODUCTION

The digital transformation of healthcare has fundamentally enhanced the management and accessibility of patient data, particularly through the implementation of Electronic Health Management Systems (EHMS). In Kenya, public hospitals have increasingly integrated EHMS to optimize healthcare service delivery, streamline operations, and improve patient care outcomes (Ouma et al., 2020; Wanyonyi et al., 2021). However, this transition has introduced a myriad of cybersecurity vulnerabilities, including data breaches, unauthorized access, and various forms of cybercrime that jeopardize the confidentiality, integrity, and availability of sensitive patient information (Davis et al., 2021). The escalating incidence of cybersecurity attacks in healthcare sectors globally emphasizes the pressing need for robust data protection mechanisms (World Health Organization, 2022).

Blockchain technology, characterized by its decentralized, transparent, and immutable ledger system, has emerged as a promising solution to address these cybersecurity vulnerabilities within healthcare systems. By eliminating single points of failure and ensuring that data alterations are detectable, blockchain presents an innovative approach to enhancing the security of EHMS (Kuo et al., 2017). The technology's capability to provide secure, verifiable, and tamper-resistant records is crucial for safeguarding patient data and maintaining stakeholder trust in the healthcare ecosystem.

This research aims to evaluate the effectiveness of blockchain technology in mitigating cybersecurity threats within EHMS in public hospitals in Kenya. Specifically, the study investigates how blockchain can address critical cybersecurity challenges, such as data breaches, hacking, and unauthorized access, which are prevalent in healthcare environments (Hassan et al., 2021). By examining the potential advantages and limitations of blockchain technology, this study aspires to establish a framework for enhancing the security of EHMS in Kenya, thereby ensuring that sensitive patient information remains protected in an increasingly digital healthcare landscape.

The significance of this study lies in its potential to inform the development of more secure healthcare information systems, which are essential for safeguarding patient privacy and enhancing the overall efficacy of healthcare delivery in Kenya. By exploring the applicability of blockchain technology within the public healthcare sector, this research could catalyze future innovations in digital health security.

II. PROBLEM STATEMENT

The increasing prevalence of cyber threats in public hospitals in Kenya presents significant challenges to the security of Electronic Health Management Systems (EHMS), which are critical for maintaining the confidentiality and integrity of sensitive patient data. Despite the deployment of various cybersecurity measures, incidents of data breaches and unauthorized access persist at alarming rates, indicating that current security protocols are insufficient to mitigate these risks. This study identifies a critical gap in the application of blockchain technology within EHMS, which offers a decentralized approach to enhance data security and reduce vulnerabilities associated with cyber threats. However, the potential adoption of blockchain technology is impeded by several barriers, including high implementation costs, inadequate digital infrastructure, and a shortage of skilled personnel. This research aims to empirically investigate the feasibility and effectiveness of integrating blockchain technology into EHMS within public hospitals in Kenya, thereby addressing the urgent need for advanced cybersecurity measures while identifying the key facilitating conditions required for successful implementation.

III. RELATED STUDIES

The integration of Electronic Health Management Systems (EHMS) in healthcare institutions has enhanced operational efficiency and improved patient care. However, this advancement has also exposed critical vulnerabilities, particularly regarding data security. The emergence of blockchain technology has been proposed as a potential solution to mitigate these vulnerabilities. This literature review explores the current cybersecurity challenges facing EHMS, the application of blockchain in healthcare, and its potential effectiveness in addressing these issues, particularly within the context of public hospitals in Kenya.

1. Cybersecurity Challenges in EHMS

The widespread adoption of EHMS in healthcare systems globally is attributed to its capacity to streamline data management, facilitate communication among healthcare providers, and enhance patient outcomes. However, numerous studies have highlighted significant cybersecurity threats associated with EHMS, especially in low-resource settings such as Kenya. Saleem et al. (2020) report that healthcare data breaches have increased in frequency and complexity, primarily targeting the extensive repositories of sensitive patient data housed in EHMS. Common cyber threats include hacking, unauthorized access, malware attacks, and data tampering. Furthermore, the healthcare sector's reliance on internet-connected systems heightens exposure to external threats (Bhuyan et al., 2021).

In the Kenyan context, Mbugua et al. (2022) note that public hospitals often grapple with outdated systems, inadequate cybersecurity infrastructure, and a scarcity of skilled personnel to manage these threats. The high sensitivity of patient data makes it an attractive target for cybercriminals. Oduor (2019) emphasizes that data breaches not only violate patient privacy but can also result in severe reputational and financial damage to healthcare institutions. Such challenges necessitate the adoption of more advanced and resilient security technologies.

2. Blockchain Technology in Healthcare

Blockchain technology has garnered attention for its potential to address data security challenges across various industries, including healthcare. At its core, blockchain is a decentralized, distributed ledger technology that ensures the integrity and security of data through cryptographic techniques. Studies by Zhang et al. (2020) and Kuo et al. (2019) elucidate key features of blockchain, such as immutability, transparency, and decentralized control, which collectively create a robust framework for data security. By ensuring that no single entity has complete control over the data, blockchain reduces the likelihood of unauthorized access and data tampering.

In healthcare, blockchain can secure patient data, ensure transparency in data sharing, and maintain the integrity of medical records (Angraal et al., 2017). Researchers such as Sharma et al. (2021) have proposed leveraging blockchain to enhance the security of EHMS by creating an immutable audit trail that tracks all access to patient data. Additionally, blockchain's implementation of smart contracts has been suggested to automate data access protocols, ensuring that only authorized personnel can access sensitive health information.

3. Effectiveness of Blockchain in Addressing Cybersecurity Issues

Various studies have examined the effectiveness of blockchain technology in mitigating cybersecurity issues within EHMS. Peterson et al. (2020) review how blockchain's decentralized nature reduces the risks associated with centralized databases, common targets for cybercriminals. By distributing data across a network of nodes, blockchain ensures that even if one node is compromised, the integrity of the entire system remains intact. This resilience is particularly valuable in environments like Kenya's public healthcare system, where resources for cybersecurity may be limited.

Furthermore, blockchain's use of cryptographic hashing enhances data security by enabling easy detection of any attempts to alter patient records (Fan et al., 2020). A study by Roehrs et al. (2019) found that blockchain significantly reduces the risk of data breaches in healthcare systems reliant on EHMS by providing a secure, immutable ledger of patient information. The technology has also demonstrated its ability to improve trust and transparency, as all transactions are recorded and verifiable by stakeholders.

However, challenges persist in implementing blockchain in public healthcare systems, especially in resource-constrained environments like Kenya. Thakur and Sharma (2021) highlighted issues such as high implementation costs, the necessity for substantial computational resources, and potential scalability problems as significant barriers to blockchain adoption. Despite these challenges, several pilot projects across various countries have showcased the feasibility of blockchain in healthcare, providing insights for its application in Kenya's public hospitals.

4. Blockchain in Kenya's Public Healthcare Sector

Research on the utilization of blockchain in Kenya's public healthcare sector remains limited, despite the country's interest in exploring digital innovations. Gichoya et al. (2022) assert that Kenya has made considerable progress in the digitization of healthcare services, with initiatives like the eHealth strategy aiming to enhance the integration of information technology in the health sector. Blockchain could complement these efforts by providing a secure infrastructure for patient data management.

Nonetheless, Muriithi and Ngugi (2023) argue that while blockchain offers substantial security advantages, its implementation in Kenya's public hospitals will necessitate overcoming systemic challenges, including a lack of digital infrastructure, limited funding, and insufficient training for healthcare personnel. These barriers underscore the need for a tailored approach that considers Kenya's unique healthcare context while capitalizing on blockchain's security benefits.

5. Research Gaps

While existing literature suggests that blockchain technology could address many cybersecurity challenges in EHMS, research focused specifically on Kenya's public healthcare sector is limited. Most studies have concentrated on blockchain applications in high-resource settings, leaving a gap in understanding how this technology can be effectively implemented in low- and middle-income countries like Kenya. Additionally, while the technical aspects of blockchain are well-documented, there is a pressing need for further exploration of the practical and policy implications of integrating blockchain into public health systems.

Blockchain technology presents a promising solution to the cybersecurity challenges faced by EHMS, particularly in resource-constrained settings such as Kenya's public hospitals. Its decentralized, secure, and transparent nature makes it well-suited to address issues like data breaches, unauthorized access, and data integrity. Nevertheless, significant challenges remain in terms of implementation, cost, and scalability, especially within the context of Kenya's healthcare system. This study aims to address these gaps by investigating the effectiveness of blockchain in enhancing EHMS cybersecurity and providing a framework for its integration into public hospitals in Kenya.

IV. METHODOLOGY

This study employed a mixed-methods research approach to investigate the effectiveness of blockchain technology in addressing cybersecurity crimes within Electronic Health Management Systems (EHMS) in public hospitals across Kenya. By integrating both quantitative and qualitative data collection and analysis techniques, the mixed-methods design aimed to provide a comprehensive understanding of the research problem (Creswell & Plano Clark, 2018).

The target population for this study consisted of IT specialists, cybersecurity experts, and healthcare professionals who were involved in the implementation and management of EHMS within public hospitals in Kenya. To ensure a robust sampling strategy, the study employed two distinct sampling methods. Firstly, purposeful sampling was utilized to select IT specialists and cybersecurity experts based on their expertise and active involvement in EHMS security (Patton, 2015). This method ensured that participants possessed the necessary knowledge and experience to provide valuable insights into the effectiveness of blockchain technology in addressing cybersecurity issues. Secondly, stratified random sampling was employed to select healthcare professionals. This approach guaranteed representation across various hospital departments, thereby enriching the diversity of perspectives and experiences captured in the study (Creswell, 2014).

In terms of sample size, the study aimed to recruit approximately 10 IT specialists, 5 cybersecurity experts, and 156 healthcare professionals. This diverse sample size was designed to ensure a broad range of insights into the effectiveness of blockchain technology in enhancing the security of EHMS in public hospitals. By including a variety of stakeholders, the study sought to illuminate the multifaceted nature of cybersecurity challenges and the potential solutions offered by blockchain technology.

Findings, Interpretation, and Discussion

Survey Results

The quantitative survey results from IT specialists and cybersecurity experts revealed critical insights into the cybersecurity landscape of Electronic Health Management Systems (EHMS) within public hospitals in Kenya. A significant 78% of respondents identified data breaches as the most prevalent cyber threat, underscoring a growing concern regarding the vulnerability of patient data. Furthermore, 64% reported frequent incidents of unauthorized access to patient records, while 56% cited malware attacks as a recurring problem. These findings highlight the urgent need for robust cybersecurity measures to protect sensitive health information.

In evaluating the current security measures, an overwhelming 82% of IT specialists indicated that existing cybersecurity strategies were insufficient to address the spectrum of emerging threats. Although firewalls and encryption were the most commonly utilized security methods, 69% of respondents believed these measures were outdated and vulnerable to increasingly sophisticated attacks. This perception emphasizes a gap between current practices and the evolving landscape of cybersecurity threats, indicating a critical need for innovative solutions.

When assessing the perceived effectiveness of blockchain technology, an impressive 87% of experts expressed confidence in its ability to enhance EHMS security. They believed that blockchain could significantly mitigate unauthorized access and data tampering, with 90% agreeing that its decentralized and immutable nature would reduce risks of data manipulation. Additionally, 77% of respondents felt that blockchain could improve auditability and enhance the traceability of data access, a crucial aspect in mitigating insider threats. These results suggest a strong belief among experts that blockchain technology holds the potential to transform cybersecurity within EHMS.

Interpretation and Discussion

The survey findings indicate a pressing need for improved cybersecurity measures within EHMS, as evidenced by the high rates of perceived cyber threats and the inadequacies of current security protocols. The significant identification of data breaches as a prevalent threat (78%) aligns with global trends, where healthcare data is increasingly targeted by cybercriminals. This perception not only reflects the actual risk but also emphasizes the need for hospitals to adopt more comprehensive and innovative security solutions, such as blockchain technology.

The fact that 82% of IT specialists believe existing security measures are insufficient points to a critical gap in cybersecurity strategies. This gap necessitates a reevaluation of current practices and a shift toward more resilient systems. The acknowledgment that firewalls and encryption are perceived as outdated (69%) suggests that healthcare organizations must invest in more advanced technologies and strategies to stay ahead of evolving threats.

The enthusiasm for blockchain technology among the experts, with 87% expressing confidence in its effectiveness, is promising. This optimism reflects a growing recognition of blockchain’s potential benefits, including enhanced data integrity, security, and transparency. The high agreement on blockchain's ability to mitigate unauthorized access and data manipulation indicates that experts view it as a viable solution to address current cybersecurity challenges. However, the transition to blockchain will require significant investment in both technology and training.

Interview Results

The qualitative interviews conducted with healthcare professionals further illuminated the concerns surrounding cybersecurity and the potential role of blockchain technology. Many participants acknowledged the risks to patient data, expressing concerns about privacy violations and the potential misuse of sensitive information. Some healthcare providers recounted personal experiences or instances of data breaches within their institutions, contributing to a pervasive atmosphere of mistrust in the current EHMS. This sentiment underscores the necessity for a secure and reliable framework to protect patient information.

Despite limited prior knowledge of blockchain technology, healthcare professionals recognized its value in ensuring data integrity and protecting privacy once it was adequately explained to them. However, they emphasized the need for comprehensive training and support for staff to facilitate the successful adoption of blockchain. This finding suggests that while there is openness to embracing new technologies, organizational readiness and training will be essential to overcoming resistance and ensuring effective implementation.

Challenges Identified

The study also identified several challenges that could hinder the adoption of blockchain technology in EHMS. A notable 88% of participants indicated that the high cost of implementation was a significant barrier to adoption. This reflects the financial constraints faced by public hospitals, which often operate on limited budgets. Additionally, many institutions lack the necessary IT infrastructure to support the integration of blockchain, further complicating the transition to more secure systems.

Another critical challenge highlighted by 65% of respondents was the lack of skilled personnel capable of managing and maintaining blockchain systems. This shortage underscores the importance of investing in training and development to build the necessary expertise within the healthcare sector.

V. CONCLUSION

In conclusion, the integration of blockchain technology within Electronic Health Management Systems (EHMS) in public hospitals in Kenya presents a promising avenue for enhancing cybersecurity, addressing the pressing challenges of data breaches, unauthorized access, and data integrity. The findings from this study underscore the inadequacies of current cybersecurity measures, with a significant majority of IT specialists expressing concern over the rising prevalence of cyber threats and the insufficiency of existing security protocols. Despite the recognition of blockchain's potential to mitigate these risks, significant challenges remain, including high implementation costs, a lack of digital infrastructure, and insufficient skilled personnel. Moreover, the mixed-methods approach revealed a strong consensus among cybersecurity experts regarding blockchain's ability to enhance EHMS security, alongside a cautious optimism from healthcare professionals who recognize the necessity of adequate training and organizational readiness for successful implementation. Overall, this research not only highlights the urgent need for innovative security solutions in Kenya's public healthcare sector but also establishes a foundation for future exploration into the practical application of blockchain technology in safeguarding sensitive patient data, ultimately contributing to the improvement of healthcare service delivery in an increasingly digital landscape.

REFERENCES

1. Angraal, S., Krumholz, H. M., & Hsieh, S. C. (2017). The role of blockchain in healthcare: A systematic review. Health Affairs, 36(10), 1754-1761. https://doi.org/10.1377/hlthaff.2017.0601

2. Bhuyan, S. S., Sethi, A., & Adhikari, B. (2021). Cybersecurity in healthcare: A review of risks, challenges, and solutions. Journal of Cybersecurity and Privacy, 1(1), 33-49. https://doi.org/10.3390/jcp1010004
3. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage Publications.
4. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). Sage Publications.
5. Davis, M., Cooper, A., & White, R. (2021). Cybersecurity risks in healthcare: A critical review of existing frameworks. International Journal of Healthcare Management, 14(1), 12-20. https://doi.org/10.1080/20479700.2020.1765762
6. Fan, K., Ma, Q., & Shen, Z. (2020). Enhancing data security in healthcare systems: A blockchain-based approach. Journal of Network and Computer Applications, 160, 102629. https://doi.org/10.1016/j.jnca.2019.102629
7. Gichoya, J. M., Ogutu, R., & Oduor, J. (2022). E-health strategies in Kenya: Progress and challenges. African Journal of Health Informatics, 5(1), 45-58. https://doi.org/10.1007/s41666-022-00114-5
8. Hassan, S. R., Al-Fuqaha, A., & Mohamed, M. (2021). The role of blockchain technology in enhancing healthcare security. Health Informatics Journal, 27(2), 146-156. https://doi.org/10.1177/1460458220901543
9. Kuo, T. T., He, Y., & Hall, K. (2017). Blockchain technology in health care: A systematic review. Healthcare, 5(2), 24. https://doi.org/10.3390/healthcare5020024
10. Kuo, T. T., Kim, H. E., & Hall, K. (2019). Blockchain distributed ledger technology for health data exchange: A systematic review. International Journal of Medical Informatics, 128, 54-67. https://doi.org/10.1016/j.ijmedinf.2019.05.017
11. Mbugua, S., Kamau, R., & Gachiri, T. (2022). Cybersecurity threats to electronic health management systems in Kenyan public hospitals. International Journal of Health Information Management, 12(2), 101-110. https://doi.org/10.1016/j.ijhim.2021.12.004
12. Muriithi, K. W., & Ngugi, E. K. (2023). Assessing the feasibility of blockchain technology in Kenya's healthcare system. Journal of Global Health, 13, 1-10. https://doi.org/10.7189/jogh.13.05002
13. Oduor, J. (2019). Data breaches in healthcare: Implications for privacy and security. Journal of Medical Internet Research, 21(4), e12256. https://doi.org/10.2196/12256
14. Ouma, M., Waithaka, P., & Nyang'aya, H. (2020). Assessing the impact of electronic health management systems on healthcare service delivery in Kenya. Journal of Health Informatics in Africa, 7(1), 1-14. https://doi.org/10.1007/s10799-020-00352-5
15. Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). Sage Publications.
16. Peterson, K. J., Eder, A., & Silvestri, F. (2020). The impact of blockchain technology on the security of electronic health records. Health Information Science and Systems, 8(1), 1-10. https://doi.org/10.1007/s13755-020-00266-y
17. Roehrs, A., de Mello, R. F., & de Souza, J. F. (2019). Blockchain technology for enhancing data security in healthcare: A review. Health Informatics Journal, 25(4), 1270-1285. https://doi.org/10.1177/1460458217711960
18. Saleem, F., Rajab, A., & Parvez, S. (2020). Cybersecurity threats and data breaches in healthcare: A systematic review. Journal of Information Security and Applications, 53, 102532. https://doi.org/10.1016/j.jisa.2020.102532
19. Sharma, R., Singh, R., & Singh, M. (2021). Utilizing blockchain technology for secure healthcare data management. Journal of Health Management, 23(2), 175-185. https://doi.org/10.1177/09720634211008479
20. Thakur, R., & Sharma, A. (2021). Blockchain technology in healthcare: A comprehensive review. Journal of Healthcare Engineering, 2021, 1-12. https://doi.org/10.1155/2021/5595364
21. Wanyonyi, K., Muli, K., & Mwale, S. (2021). The effectiveness of electronic health records in improving patient care in Kenyan public hospitals. African Journal of Health Sciences,

34(2), 115-126. https://doi.org/10.4314/ajhs.v34i2.2

22. World Health Organization. (2022). Cybersecurity in health: A global perspective. https://www.who.int/publications/i/item/cybersecurity-in-health-a-global-perspective
23. Zhang, P., Malik, R., & Zhang, Z. (2020). A review on blockchain technology in healthcare: Applications and challenges. Health Information Science and Systems, 8(1), 1-10. https://doi.org/10.1007/s13755-020-00263-1