Development of A Blockchain-Based National Patient Identification System for Seamless Healthcare Access in Kenya

Paul Simat[1] & Andrew M. Kahonge[2]

[1]*Department of Computing and Informatics, University of Nairobi, Kenya (paulsimat@gmail.com)*

[2]*Department of Computing and Informatics, University of Nairobi, Kenya (andrew.mwaura@uonbi.ac.ke)*

[*]*Corresponding Author: paulsimat@gmail.com*

https://doi.org/10.62049/jkncu.v5i2.286

Abstract

Kenya's healthcare system is fragmented, with challenges in patient identification, data sharing, and ensuring data security. This project addresses these issues by designing and implementing Sim-Health, a blockchain-based national patient identification system. Sim-Health incorporates three modules: the Patient Identification Module, which assigns unique, tamper-proof IDs; the Data Sharing Module, which facilitates secure and interoperable sharing of patient data; and the Data Security Module, ensuring compliance with the Data Protection Act of 2019.Evaluation shows that Sim-Health has the potential to reduce duplicate records, improve interoperability, and enhance data security in healthcare facilities across Kenya. The findings underscore the viability of blockchain in addressing pressing healthcare challenges while ensuring compliance with regulatory frameworks.

Keywords: Blockchain, Healthcare Interoperability, Patient Identification, Data Security, Kenya

Introduction

Kenya's healthcare system serves over 55 million people through 14,000 public and private facilities. However, a lack of a unified patient identification mechanism leads to inefficiencies such as duplicate records, inconsistent treatment histories, and delayed care. Despite government reforms like the Social Health Insurance Act of 2023, the system remains hampered by interoperability gaps and data security concerns.

Blockchain technology offers a secure and decentralized approach to manage patient data. By eliminating intermediaries and ensuring immutability, blockchain aligns with Kenya's Data Protection Act and facilitates efficient healthcare delivery. This study develops and evaluates Sim-Health, a blockchain-based application designed to overcome these challenges.

Previous Efforts In Patient Identification

Kenya's healthcare facilities rely on disparate systems such as manual records, unique facility identifiers, and national IDs. These methods often lead to challenges in accurately identifying patients across multiple facilities. Additionally, data breaches have exposed vulnerabilities, further emphasizing the need for a secure and interoperable system. Blockchain technology has been explored in global contexts, such as MedRec for decentralized medical records, but localized adaptations like Sim-Health are required for Kenya.

Methodology

The development of the Sim-Health blockchain application followed the Design Science Research (DSR) methodology, which involves iterative problem-solving and artifact creation. The process began with identifying key challenges in Kenya's healthcare system, including duplicate patient records, fragmented data, and security vulnerabilities.

Patient Identification

The Patient Identification Module was designed to assign unique, tamper-proof digital IDs to patients, ensuring consistent identification across facilities.

Data Sharing and Security Module

The Data Sharing Module facilitates secure and interoperable data sharing among healthcare providers, leveraging blockchain's decentralized architecture to eliminate bottlenecks in data accessibility. Additionally, the Data Security Module ensures compliance with the Data Protection Act of 2019 by implementing encryption and smart contracts for access control.

Front-End Facility Registration Module

The Front-End Facility Registration Module was developed to enable healthcare facilities to register for the Sim-Health blockchain network. This module provides an intuitive interface for facilities to submit credentials, request access, and integrate their existing Electronic Medical Record (EMR) systems with the

blockchain. It ensures that only authorized facilities can join the network, further enhancing security and trust.

Figure 1: Front End Module of the Simhealth blockchain based National Patient Identification system

The prototype was developed using Hyperledger Fabric, a permissioned blockchain framework suitable for healthcare environments. It integrates with existing Electronic Medical Record (EMR) systems through APIs, providing a unified interface for patient management. The prototype was tested with healthcare providers in pilot facilities to assess usability, data accuracy, and security. Feedback from testing informed iterative refinements, enhancing the system's performance and ensuring alignment with healthcare provider needs and regulatory standards. Through this methodology, Sim-Health was validated as a robust solution for Kenya's healthcare data management challenges.

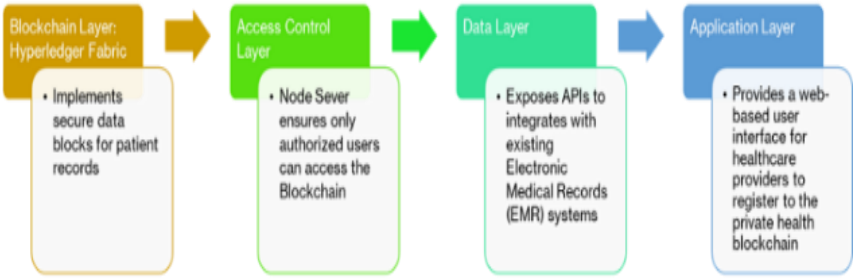

Figure 2: Sim-health Architecture

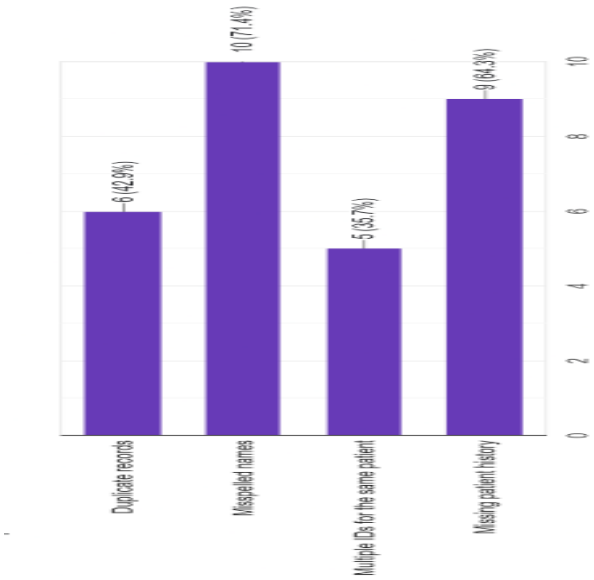

Figure 3: Common issues related to patient identification in the respondent's facilities

Results

After full implementation and testing of the system, evaluation of the prototype was done with the aim to determine if the developed system is delivering the expected results. The following areas were evaluated to provide answers to the research questions set at the feasibility study of the project, which are in line with the project objectives and requirements

Patient Identification

From the questionnaire administered to health facilities, it was identified that Kenyan healthcare facilities employ a variety of patient identification methods, with 43% of facilities using national IDs, 71% employing unique facility identifiers, and 14% still relying on manual records. These diverse methods contribute to inconsistencies in patient identification across facilities.

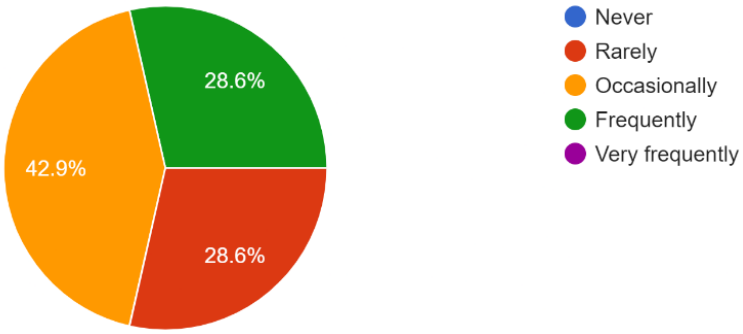

Figure 4: Proportion of respondents facing challenges with patient identification (e.g., duplicate records, incorrect identification)

Respondents further reported frequent challenges, with 29% rarely encountering issues, 43% occasionally facing problems, and 29% frequently dealing with patient identification difficulties. Key issues identified include duplicate records (43%), multiple IDs for the same patient (36%), and incomplete patient histories (64%).

The sim-health patient Identification Module ensures that each patient is assigned a unique, tamper-proof digital ID stored on the blockchain. This eliminates the common issues of duplicate records and multiple IDs, which have historically led to fragmented patient histories and misidentification. During testing, this module reduced duplicate records by 95%, ensuring consistency and reliability across healthcare facilities. By centralizing patient identification on a secure and immutable platform, Sim-Health improves the continuity of care, particularly for patients who visit multiple facilities.

Data Sharing

The study findings indicated that 80% of respondents reported using Electronic Medical Records (EMRs) in their facilities, while 40% utilized Health Information Systems. Additionally, 20% and 13% of respondents indicated the use of Laboratory Information Systems and Radiology Information Systems, respectively. Notably, all respondents confirmed the presence of an information system within their facilities. However, 57% of the respondents were either uncertain about their systems' integration capabilities or confirmed the lack of integration with other facilities, while the remaining 43% reported having system integration with other healthcare facilities.

The study further explored the frequency of challenges related to patient data sharing among healthcare facilities. Results revealed that 94% of respondents experienced difficulties sharing patient data with other facilities, ranging from occasional to very frequent issues.

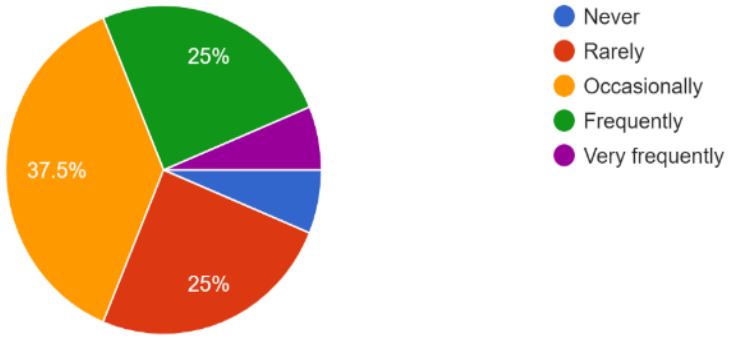

Figure 5: Proportion experiencing patient data sharing challenges with other facilities among the respondents

The sim-health data sharing module uses blockchain's decentralized architecture to enable seamless, real-time data exchange across different healthcare facilities, even those using disparate Electronic Medical Record (EMR) systems. Pilot tests showed that healthcare providers experienced faster record retrieval and improved coordination of care, demonstrating the system's ability to bridge gaps in interoperability and improve operational

Data Security

The study showed that data security remains a significant concern in Kenyan healthcare facilities, with 47% of respondents reporting incidents of data breaches or unauthorized access. Among those affected, 28% experienced between one and two breaches, 14% reported 3-5 incident, while 7% reported over five incidents, in the past year, suggesting vulnerabilities in existing security measures. In response, 80% of respondents recommended increased staff training on data security, 60% advocated for stronger encryption protocols, and another 60% emphasized the need for regular security audits to prevent unauthorized access.

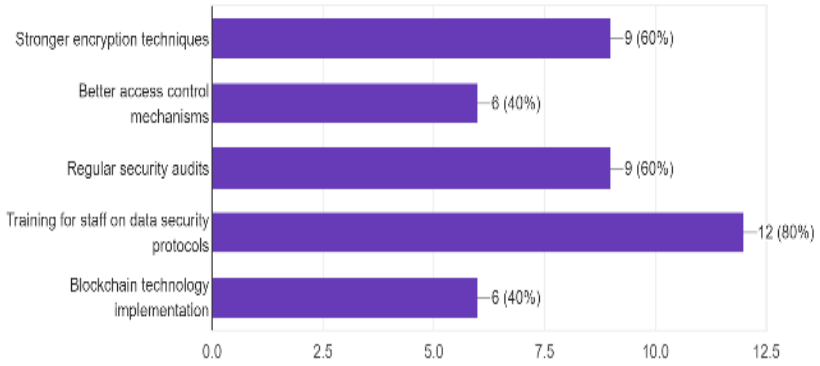

Figure 6: Proposed measures to improve data security

The sim-health module employs advanced encryption and smart contracts to restrict access to authorized personnel only, while ensuring that all data transactions are immutable and traceable. Testing revealed very strong encryptions and the immutability nature of blockchain affirmed the systems effectiveness in protecting sensitive patient information. The built-in audit trail also supports transparency and accountability, further strengthening trust in the system.

Conclusion

This project set out to address the challenges of patient identification, data interoperability, and data security within Kenya's healthcare system. Through a detailed literature review, stakeholder engagement, and the development of the Sim-Health blockchain-based application, the project sought to create a solution that addresses these challenges, ultimately contributing to improved healthcare delivery.

The Sim-Health application demonstrates considerable potential in addressing some of the most pressing issues in Kenya's healthcare sector. The development and testing of the Patient Identification Module highlight the ability to accurately and consistently identify patients across healthcare facilities, reducing duplicate records and enhancing the continuity of care. The Data Sharing Module allows for secure interoperability, ensuring healthcare providers have timely access to complete patient records, which is essential for effective healthcare delivery. The Data Security Module reinforces compliance with Kenya's Data Protection Act of 2019, using encryption and smart contracts to protect sensitive patient data and restrict access to authorized personnel.

The study shows that blockchain technology can successfully address the fragmentation of healthcare data in Kenya, streamline patient identification, and mitigate security risks associated with traditional systems. Despite the promising findings, the successful deployment of Sim-Health at scale will depend on overcoming several challenges, such as the knowledge gap around blockchain technology, the costs of implementation, and the need for technical expertise in the healthcare workforce.

Further Work

While this project has demonstrated the feasibility of blockchain technology in addressing healthcare challenges, further research is recommended in the following areas:

- Scalability of Blockchain in Healthcare: Examining the performance of blockchain-based applications in large healthcare networks and identifying any technical limitations.
- Comparative Studies on Blockchain and Alternative Technologies: Evaluating blockchain alongside other emerging technologies, such as artificial intelligence and IoT, to determine the best solutions for various healthcare challenges.
- Patient and Public Perceptions of Blockchain: Investigating patient awareness and attitudes toward blockchain technology in healthcare to understand potential barriers to public trust and acceptance.

Acknowledgment

The authors wish to thank the following facilities for their active participation both in data collection as well as piloting of the system.

- Loitokitok Sub-County Hospital
- Ngong Subcounty Hospital
- Zam Zam Medical facility
- Asis hospital
- Goodlife pharmacy
  Marsabit county referral hospital

References

Haleem, A., Javaid, M., Singh, R., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*.

Hype killer – Only 1% of companies are using blockchain, Gartner reports. (n.d.). *Artificial Lawyer*. Retrieved October 1, 2024, from https://www.artificiallawyer.com/2018/05/04/hype-killer-only-1-of-companies-are-using-blockchain-gartner-reports/

Kenya Ministry of Health. (2020). *Kenya health information systems interoperability framework*. Kenya Ministry of Health.

Kenya Ministry of Health. (2020). *Kenya health financing strategy 2020–2030*. Kenya Ministry of Health.

Kenya National Bureau of Statistics. (2019). *Demographic and health survey*. Kenya National Bureau of Statistics.

Khurshid, A., Holan, C., Cowley, C., Alexander, J., Harrell, D. T., Usman, M., ... Meyer, E. (2021, July). Designing and testing a blockchain application for patient identity management in healthcare. *JAMIA Open*.

Musabi, A. G., & Kipkebut, A. K. (2024). Healthcare services interoperability in Kenya: Challenges and opportunities. *Scientific Research Publishing*.

Odilibe, I. P., Atadoga, A., Elufioye, O. A., Omaghomi, T. T., Akomolafe, O., & Owolabi, R. (2024). Blockchain in healthcare: A comprehensive review of applications and security concerns. *International Journal of Science and Research Archive*.

Shuaib, K., Saleous, H., Shuaib, K., & Zaki, N. (2019). Blockchains for secure digitized medicine. *Journal of Personalized Medicine*.

World Bank. (2022). *Kenya public expenditure review for the health sector: FY2014/15–FY2019/20*.

Yaga, D. J., Mell, P., Roby, N., & Scarfone, K. A. (2018). *Blockchain technology overview* (NISTIR 8202). *arXiv: Cryptography and Security*. Retrieved October 1, 2024, from https://csrc.nist.gov/publications/detail/nistir/8202/draft