BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING

COMPUTER SCIENCE DEPARTMENT



IMPLEMENTATION OF A SECURE ELECTRONIC HEALTH RECORD (EHR) SYSTEM USING BLOCKCHAIN TECHNOLOGY. Case Study: Zimbabwe Hospitals.

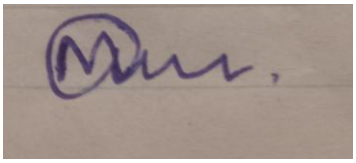
BY MERCY MAGARA

B221509B

SUPERVISOR MR MLANGANISO

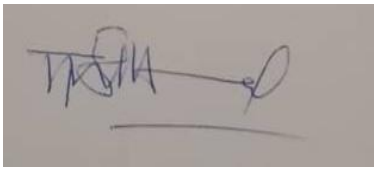
APPROVAL FORM

The undersigned certify that they have supervised the student Mercy Magara in the research dissertation entitled “Implementation of a secure electronic health record (EHR) system using blockchain technology”. Case Study: Zimbabwe Hospitals which was submitted in Partial fulfilment of the requirements for the Bachelor of Computer Science Honors Degree of Bindura University of Science Education.



……. ……...… …29…/……07/…26…..

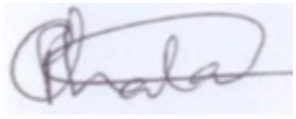
STUDENT SIGNATURE DATE



Mr Mhlanganiso

……... ……. …26…/……06…/…26……

SUPERVISOR SIGNATURE DATE



… ..Mr Chaka.....…..…26/06/26…….. CHAIRPERSON

SIGNATURE

ABSTRACT

Safeguarding patient data is a prerequisite for safe, trustworthy healthcare delivery even in low-resource settings like Zimbabwe where fragmented, insecure and inefficient patient health records management have led to data breaches and leakage. This research addressed this critical issue by developing a fortifying layer of tamper-evident, secure, decentralized electronic health record system using proof-of-work consensus mechanism (POW), python and Cryptographic hashing (SHA-256) for data integrity and authenticity. An experimental Agile design was used for iterative prototyping. Results show that the proof-of-work architecture successfully enabled strong tamper evident record storage, secure data sharing, offline synchronization (tailored for developing countries) and real time security alerts. Approximately 90% of test users could operate the system without assistance for data submission and retrieval. I recommend that future studies need to aim at implementing a Hybrid Consensus Supplementing PoW to reduce computational overhead and transaction confirmation time and enhance with Zero-Knowledge Proofs which allows verification of patient data without exposing the full record.

DEDICATION

This project is dedicated to the patients of Zimbabwe whose medical history was lost, leaked, or held hostage by broken systems especially those in rural clinics and low-resource wards. May this work bring you a future where your health data is never again a source of fear, but a foundation of trust.

ACKNOWLEDGEMENT

I would like to express my deep sense of gratitude and convey thanks to all the individuals and organizations for their support and contributions to the completion of my dissertation. Firstly, I am deeply grateful to my supervisor, Mr Mhlanganiso, for his valuable scholarly guidance and critical feedback through the whole project. Acknowledgement to the Bindura University at large for providing the academic environment that helped completion of different chapters of this project and also provision of necessary resources and infrastructure. Last, but not least, I would like to thank my family members for their constant and unwavering support towards my education and for their steadfast love and above all, I thank Almighty God for the strength and perseverance to complete this research.

Contents

APPROVAL FORM 2

DEDICATION 4

ACKNOWLEDGEMENT 5

DEFINITION OF TERMS 9

1.1 INTRODUCTION 9

1.2 BACKGROUND OF THE STUDY 10

1.3 STATEMENT OF THE PROBLEM 11

1.4 RESEARCH OBJECTIVES 12

1.5 RESEARCH QUESTIONS 12

1.6 RESEARCH HYPOTHESIS 12

1.7 SIGNIFICANCE OF THE STUDY 13

1.8 ASSUMPTIONS 13

1.9 LIMITATIONS 13

1.10 SCOPE / DELIMITATION OF RESEARCH 14

CHAPTER 2 15

2 .1 INTRODUCTION 15

Current Health Record Management Methods in Hospitals and Clinics 15

2.2 RELEVANT THEORIES 15

2.2.1 INFORMATION SECURITY TRIAD (CIA TRIAD) 15

2.2.2 TRUST ENGINEERING THEORY 16

2.2.3 PRINCIPAL-AGENT THEORY 16

2.2.4 Synthesis of Theoretical Foundations 17

2.3 REVIEW ON HEALTH RECORD MANAGEMENT MODELS IN OTHER COUNTRIES 17

Table 2.3.1: Comparative Analysis of Existing Health Record Management Models 17

2.3.1 DETAILED ANALYSIS OF SELECTED MODELS 23

2.4 SYNTHESIS OF LITERATURE REVIEW FINDINGS 28

2.4.1 Security and Privacy: Documented Patterns and Limitations 28

2.4.2 Trust and Security Architecture in Health Information Tools 28

2.4.3 Infrastructure Dependence. 30

2.4.4 African Implementation Realities 31

2.4.5 IDENTIFIED RESEARCH GAP 32

2.5.3 Contribution of the Proposed Research 34

2.6 CHAPTER SUMMARY 35
CHAPTER 3 37
3.0 INTRODUCTION 37
3.1 RESEARCH DESIGN 37
3.1.1 EXPERIMENTAL RESEARCH DESIGN 37
3.2 POPULATION AND SAMPLE 38
3.2.1 Sample Size 39
3.3 RESEARCH INSTRUMENTS 39
3.3.1 Reliability and Validity 40
Validity 40
3.3 .2 Data Collection Process 41
3.3.3 Ethical Consideration 42
4.0 SYSTEM DOCUMENTATION 43
4.1 HARDWARE REQUIREMENTS 43
4.1.2 SOFTWARE REQUIREMENTS 43
4.1.4 SYSTEM DEVELOPMENT TOOLS 44
4.1.5 AGILE DEVELOPMENT METHODOLOGY 44
4.1.6 WHY I CHOOSE AGILE METHODOLOGY 44
4.1.8 SYSTEM DESIGN 45
FLOW CHART 46
4.2 DATA FLOW DIAGRAMS 47
4.2.4 AUDIT LOGS 50
CHAPTER 4 - DATA PRESENTATION, ANALYSIS AND INTERPRETATION 52
4.1 Introduction 52
4.1.1 System Security and Performance Metrics 52
Figure 4.1.2 53
4.1.3 Transaction Throughput (TPS) 53
4.2 User Evaluation Metrics 54
4.3 Response Rate 54
FIG 4.3.1 54
4.3.2 Pre-Implementation Analysis (Baseline Findings - challenges in existing systems) 55
FIGURE 4.3.3 55
4.3.4 System Usability 55

4.3.7 Confidence in Data Security. 56
FIGURE 4.3.7 56
4.3.8 Interpretation 57
4.3.9 Post-Implementation Analysis (Experimental Group) 57
4.0 Improvement in Data Security 57
Figure 4.1 57
FIGURE 4.2 57
4.3 Improvement in Data Security 58
4.4 System Performance (From Logs) 58
4.5 Control Group Analysis 58
4.6 Comparative Analysis (Experimental vs Control Group) 59
FIGURE 4.7 59
4.8 Qualitative Analysis (Interviews) 59
4.9 Interpretation 60
4.9.4 Discussion of Findings 62
4.9.5 Inferential Statistical Analysis - Paired Sample t-Test 62
4.9.6 Interpretation 63
5.0 CHAPTER SUMMARY 63
CHAPTER 5: CONCLUSION AND RECOMMENDATIONS 64
5.1 Introduction 64
5.2 Major Conclusions Drawn 64
5.3 Recommendations 65
5.4 CHAPTER SUMMARY 66
5.5 REFERENCES 68

CHAPTER 1: PROBLEM IDENTIFICATION

DEFINITION OF TERMS

EHR – Refers to a digital system that collects, processes, stores, and manages patient health information, that is patient's clinical history which include diagnoses, medications, treatment plans, and lab results, allowing healthcare providers to access and share information efficiently.

BLOCKCHAIN TECHNOLOGY - is a distributed electronic ledger system that keeps track of transactions across several computers, guaranteeing that once data is recorded, it cannot be changed without network consensus.

TRANSPARENCY - Refers to the clarity and openness in processes, communications, and data sharing.

PROOF OF WORK(PoW) - a decentralized consensus technique, to securely add new blocks to the ledger and verify transactions. To solve challenging cryptographic riddles, network users, referred to as miners, must invest a substantial amount of computational power.

1.1 INTRODUCTION

The Zimbabwe healthcare sector faces significant challenges in the secure management patient data, like many developing countries. This is because medical institutions rely on fragmented or paper-based record-keeping systems, leading to high privacy concerns (Chilunjika, Uwizeyimana, 2024). This problem hinders the continuity of care and limit the ability to make informed medical decisions. According to (Owolabi & Owolabi, 2025); the rapid digital transition in healthcare calls for safer and efficient tool that can be used to retain store health records for patients.

Blockchain is a technology that is based on decentralization and immutability to solve these challenges meaning that the problems concerning the security and connectivity in medical information systems become resolved (Reegu et al., 2022). Storing Electronic Health Records on a distributed system like blockchain technology can help to ensure that there is data integrity which can somehow improve interoperability among healthcare institutions enhancing patient

trust through secure and verifiable record-keeping. This research proposes the designing of a blockchain-based tool for secure EHR storage and access management in healthcare facilities, implementing the tool to see if it resolves the problem we are facing and evaluating it according to how it works.

1.2 BACKGROUND OF THE STUDY

Electronic Health Records (EHRs) refers to patient's health histories or clinical data that are maintained over time and it allows healthcare professionals to access and distribute information efficiently (Weiskopf et al., 2013). However, current centralized systems used in Zimbabwe's healthcare facilities expose data to several vulnerabilities such as unauthorized access, tampering, and loss due to system failures or cyber-attacks. Hospitals and clinics often operate independently, there is limited interoperability and no unified mechanism for secure data exchange. Comprehensive reviews confirm that blockchain improves security of health records, addressing core challenges identified in Zimbabwe's health information systems. Security is categorized into three subcategories according to CIA Triad which are availability, integrity, and confidentiality. Confidentiality refers to the fact that the medical information will only be permitted to be used or being retrieved by entitled users only. This prevents unsanctioned use of private data even the viewing of that data. Integrity can be defined as a way in which the patient information must be consistent, cannot be modified or destroyed hence correctness and availability means that EHRs are accessed timely to permitted users where and when the user need to access it meaning that when the data is not known when the user wants it, there is no use in storing it (Al Mamun et al., 2022).

Blockchain technology states that information is enciphered so that it can be retrieved or utilized to authorized individuals hence enhancing the existing security framework (Rejeb et al., 2021). Each medical record or transaction stored on the blockchain is time-stamped, traceable, and immutable, ensuring that records cannot be modified without detection. Blockchain technology is still not widely used in Zimbabwe's healthcare industry. This technology is not widely used for managing health information, despite ongoing talks and experimental projects.

The need to guarantee confidentiality, compatibility, and accessibility, technological advances like blockchain have the potential to completely transform the management of healthcare records (Antonio & Nhapi, 2022). Integrating blockchain with the Healthcare IoT improves up to the minute data security and interoperability (IoMT & Blockchain study, 2025). This project aims to develop an invulnerable, efficient, and transparent tool for archiving and transferring patient information among healthcare stakeholders.

1.3 STATEMENT OF THE PROBLEM

Data pertaining to personal health is highly vulnerable to misuse, and this data includes secondary data that is consistent with the original goals of gathering. These risks are not new, to be sure (Saki, 2024). There is patient data breaches and leakage due to highly fragmented, insecure and inefficient current methods of managing patient health records. Most healthcare facilities use local databases or manual record-keeping, which makes it difficult to maintain data consistency and confidentiality. Weak data protection enforcement in Zimbabwe undermines patient confidentiality in electronic health record systems (Saki, 2024). Unauthorized access and data breaches is a great challenge which can lead to limited trust among patients considering how their health information is handled in health care services.

The absence of a distributed, immutable and transparent tool for storing and transferring Electronic Health Records limits healthcare efficiency and patient trust. This opens a gap or a pressing need to compose a health immutable tool which enhances data security, integrity, and interoperability among healthcare institutions. Taking advantage of decentralized ledger features, medical field would be transformed into a more impactful framework for personal health records for patients unlike traditional systems guarantees that patient information cannot be modified, destroyed or be available to unpermitted individuals only to authorized parties, therefore improving the patience trust, coordination and reliance from the healthcare delivery (Daraghmi, et al., 2019).

1.4 RESEARCH OBJECTIVES

1. Analyze current methods in patients' health record management used by healthcare institutions.
2. To design a blockchain-based tool guaranteed for safer retention and transferring of Digital Patient Health Records for hospitals and clinics.
3. Evaluate the capability of the recommended tool with respect to security, scalability, and efficiency.

1.5 RESEARCH QUESTIONS

1. Identify the present challenges associated with managing Digital Health Records in medical centers?
2. In what manner can the distributed ledger technology be used to improve security coupled with interoperability of Electronic Health Records?
3. What design tool best suits safer storage and transferring of patient data when utilizing a distributed ledger?
4. How efficient, scalable is the proposed blockchain-based tool compared to traditional EHR systems?

1.6 RESEARCH HYPOTHESIS

Null Hypothesis (H0)

Adopting a decentralized system for digital patient records does not significantly improve the integrity and security of patient data compared to existing centralized systems.

Alternative Hypothesis (H1)

Adopting a decentralized system for digital patient records significantly improves integrity and security of patient records compared to existing centralized systems.

1.7 SIGNIFICANCE OF THE STUDY

This project will provide a practical tool for applying blockchain technology to healthcare in Zimbabwe. It will bridge the gap between traditional centralized record systems and modern decentralized health data management solutions. The results will help policymakers, healthcare administrators, and IT professionals on how blockchain can be adopted for national healthcare data reform, contributing to the government's digital transformation initiatives and SDG 3 (Good Health and Well-being).

1.8 ASSUMPTIONS

1. Healthcare professionals will be ready to accept and use a blockchain-based EHR tool, offered adequate training and resources.
2. The existing technological infrastructure in healthcare facilities, while limited, will be sufficient to support the initial implementation of a blockchain system.
3. Stakeholders, including healthcare providers and policymakers, will recognize the benefits of blockchain technology and support its integration into the current healthcare system.
4. Data privacy and security regulations will be adhered to during the design and implementation of the blockchain system, ensuring compliance with national healthcare standards.

1.9 LIMITATIONS

1. Resistance to technology adoption by healthcare professionals due to lack of adequate fear of learning new things or of the unknown, making it challenging to ensure that all staff members are on board with the new tool.
2. The blockchain technology is very promising but is still relatively new to many in the healthcare sector hence its complexity can lead to challenges in understanding and utilizing it effectively, both for IT staff and healthcare providers.

3. Transforming from existing paper-based or centralized electronic systems to a new tool may involve significant data migration efforts. Ensuring data accuracy, integrity, and completeness during this process can be challenging and time-consuming.

1.10 SCOPE / DELIMITATION OF RESEARCH

The project will be conducted within the healthcare facilities in Zimbabwe, including Mashonaland Central Hospitals and selected private clinics. The research will focus mainly on formulating, implementation of a decentralized tool which enhance the security of patient records. Data collection will involve interviews with healthcare IT personnel, nurses, and doctors to understand existing challenges and system requirements.

CHAPTER 2

2 .1 INTRODUCTION

Current Health Record Management Methods in Hospitals and Clinics

Adopting digital technologies in medical facilities has transformed how the data of patients is handled or managed, allowing their records to be more safe, along with being accessible of medical services for example, the development of secure Electronic Health Record (EHR) tool gave a critical transition on the patient data is storing, transferring and accessing across healthcare facilities. The chapter below studies how the available theoretical literature in collaboration with empirical literature which are significant to the implementation of EHR tool, with particular attention to the need for a block chain tool which addresses security and interoperability problems in resource-constrained settings such as Zimbabwe's public and private hospitals.

2.2 RELEVANT THEORIES

Several theoretical frameworks lead to the need for designing and implementing a secure decentralized tool leveraging block chain technology. Below show these theories providing a lens through which to understand data security requirements in the health sector, specifically, to Zimbabwe.

2.2.1 INFORMATION SECURITY TRIAD (CIA TRIAD)

According to (Goodman & Rowland, 2020), secure information systems must ensure three core principles which are availability of data, data being confidential, and integrity of data. Confidential data states that accessibility of patient data is only to permitted people, for data to be integral, it must be accurate, complete and protected from unauthorized modification and lastly, availability means real time accessibility of patient data when it is in need of by permitted users. The research was more concerned on the isolation of the CIA triad features so that we detect breaches or gaps to patient data security, hence providing a rigorous methodology for assessing security vulnerabilities in data systems. Block chain is capable of providing cryptographic controls and audit trails that closes gap documented issues like porous security and unauthorized access in current systems. The availability principle must be carefully considered in

Zimbabwe's infrastructure context, where unreliable electricity and internet connectivity could limit access to block chain-based records, potentially requiring offline-capable designs or hybrid approaches.

2.2.2 TRUST ENGINEERING THEORY

Trust engineering, as developed by Gefen et al. (2003) and extended by Ba and Pavlou (2002), offers critical insights into how digital health platforms can systematically design features that foster user confidence among patients, healthcare providers, and administrators. This theoretical stream draws on institutional trust theory (Zucker, 1986), which distinguishes between characteristic-based trust derived from shared attributes like patients and doctors from the same community, process-based trust: derived from repeated positive interactions over time and institution-derived trust which is generated from formal mechanisms in coherence with the structural assurances.Blockchain's cryptographic verification ensures that only authorized healthcare workers with verified credentials can access or modify patient records, addressing documented concerns about unauthorized access in Zimbabwean health facilities .McKnight et al. (2002) long drawn out the context by disclosing that relying on beliefs which are ability perception , integrity and benevolence lead to willingness to depend on the system, which in turn determine willingness to share sensitive information ,a critical outcome for EHR adoption. Current contributions by Hawlitschek et al. (2016) have studied the "trust paradox" in sharing economy platforms, stating that while trust is important, excessive verification requirements can create friction that reduces participation.

2.2.3 PRINCIPAL-AGENT THEORY

The superior assign the work to an agent, creating threats of in which the agent has more information known as information asymmetry and the person in which work was delegated may not act in the principal's best satisfaction. Hoffmann and Thommes (2020) apply principal-agent theory to address information asymmetry and misaligned incentives between parties. In Zimbabwe's fragmented health landscape consisting of patients, public hospitals, private providers and government agencies, information asymmetry is common. Block chain-based EHR can serve as a trusted intermediary by yielding a guaranteed, tamper resistant or unalterable tool which can be accessible to all permitted individuals. This reduces information asymmetry, minimizes disputes over treatment histories and insurance claims and it improves how

accountable health care professionals are across the healthcare system. This creates a transparent and unaltered records of all data access and modifications, block chain aligns incentives and builds trust among everyone who may have competing interests.

2.2.4 Synthesis of Theoretical Foundations

These theoretical perspectives collectively inform the design of a block chain EHR tool that is technically strong as informed by the CIA Triad security framework(Goodman ,Rowland 2020); security-enhanced by addressing documented vulnerabilities in Zimbabwe's current systems and trust-enabling (addressing Principal-Agent information asymmetry (Hoffmann , Thommes, 2020).Together, they provide a comprehensive framework for implementing a secure, acceptable, and sustainable block chain-based EHR tool in Zimbabwean hospitals.

2.3 REVIEW ON HEALTH RECORD MANAGEMENT MODELS IN OTHER COUNTRIES

This section examines existing health record management documented in the academic literature. The review extents diverse geographical contexts and methodological approaches, with particular consideration to implementations that address data security, interoperability and technological accessibility underlying the proposed block chain-based EHR tool for Zimbabwean hospitals.

Table 2.3.1: Comparative Analysis of Existing Health Record Management Models

Cites	Model	Country of implementation	Strengths	Weaknesses
1. Alnashmi et al., 2022)	Mixed paper + partial HER	Kuwait : Government, private, and oil-sector hospitals	Ongoing digitization; some improved accessibility of records	43% of hospitals use paper-based recording. weak national regulation, standardization, privacy and retention practices.

2. (Sharma et al., 2023)	Ayushman Bharat Digital Mission (ABDM).	India	Unified longitudinal patient history. improved healthcare accessibility for rural populations.	High risk of data leaks on public-facing servers. Susceptibility to large-scale cyberattacks and state-sponsored espionage.
3.Tutty et al. (2019)	Decentralized Multi-vendor EHR (Proprietary)	USA	clinical workflow automation. robust decision support. extensive population health reporting.	Susceptible to phishing, insider threats, and ransomware due to complex vendor integrations. High-income countries face mostly output barriers such as a lack of data security especially with the emerging use of AI and Machine Learning.
4.(Semenzin et al., 2022)	Nationwide Centralized e-Health Record (KSI Blockchain Integration).	Estonia	100% population coverage; high data portability; real-time access for patients and providers.	Insider Threats: Vulnerable to unethical access or data leaks by authorized staff with valid credentials as emphasized by (Vaiknemets et al. (2019).

5. Fraser,.et al 2024	Electronic Health Record (EHR) systems based on the OpenMRS platform.	Rwanda	High data completeness (98.4%) and improved data recording with clinical alerts.	Variability in data quality, technical issues, and potential alert fatigue.
6. (Adedeji et al., 2022)	Paper records plus pilot/partial EHRs	Nigeria	Reduced replication of patient records. Real time access of patients' records. Enhanced tracking of electronic medical data which are clinic attendance and immunization history.	Reduced human capacity, brain drain, lack of enforcement of legislation and policies. Insufficient investment financially Due to corruption. Lack of infrastructure.
7.(Ngugi et al., 2021)	Kenya EMR	Kenya	Enhanced access to patient information reduced documentation	High procurement/maintenance costs, poor electricity/internet, limited user computer

			errors/redundancy , streamlined clinical workflows	skills, resistance to change, lack of robust infrastructure
8.Tayler, Kazembe (2025) Derksen et al., 2025)	Patient-held paper records plus EMaR.	Malawi	Portable and decentralized, allowing access to patient history across different facilities. Improves data quality, completeness, and consistency. High perceived usefulness for improving healthcare delivery .	Illegible handwriting and inconsistent Poor data quality, storage issues, and data loss. Low patient literacy and lack of privacy hinder effectiveness. Technology alone is insufficient; success depends on social and contextual factors. Requires reliable power, internet, and infrastructure .
9.(Asiedu et al., 2025)	Ghana Lightwave Health Information Management System (LHIMS)	Ghana	Improves patient workflows; enhances resource tracking	Interoperability gaps with national systems; data duplication challenges.

10.Madziwa PK & Masuku M (2024); Saki O (2024); Cyber and Data Protection Act (2021)	Impilo electronic health records + paper based Legal framework now mandates data protection standards.	Zimbabwe	Streamlines clinical workflows and improves information sharing among practitioners. Enhances decision-making at the point of care. Blockchain solution would align with 2021 Data Protection Act requirements for security and consent.	Faces infrastructure limitations, high staff turnover, and slow response times during periods of high patient volume. High data privacy insecurity (Saki O (2024).
11.Zerfu et al., 2025)	DHIS2-based national system	Ethopia	Aggregate data platform for health system monitoring. Enhances accountability and data quality; streamlines reporting	Interoperability issues; sustainability concerns due to funding gaps.
12. (Azaria et al., 2016)	MedRec (MIT)	USA	Decentralized record	Data synchronization difficulties Early-stage

			management system using block chain. Patients get comprehensive, immutable log of medical data across providers. Modular design integrates with providers' existing local data storage .	prototype with limited real-world testing Relies on Proof of Work which has high energy consumption
13.MrC (2025)	Medical record Chain System	Conceptual Framework	Returns data ownership to patients; temporary permission grants; bridge interface requires no changes to existing systems; smart contracts for access control; incentivizes adoption through research data access.	Conceptual/system design stage; implementation challenges not documented; dependent on voluntary institutional participation

2.3.1 DETAILED ANALYSIS OF SELECTED MODELS

1. Alnashmi et al. (2022) – Mixed Paper + Partial EHR (Kuwait)

Alnashmi and colleagues analyses the adoption digital health records in Kuwait's three leveled hospital system consisting of private, government and oil-sector facilities. Their findings acknowledged that a transformational landscape where electronic based recording has enhanced record accessibility in some facilities and somehow there is still 43 percent of medical facilities that remain using the paper-based approach. This mixed-model context bears critical semblance to our situation in Zimbabwe, in which the Impilo electronic health record system coexists with extensive paper-based record-keeping practices documented by Madziwa and Masuku (2024).

The challenge that was identified was the absence of retention policies which are inconsistent, national standardization and weak regulatory oversight created privacy insecurities, with different health care facilities adopting different standards to patient data. The Kuwaiti experience underscores that technical solutions alone are not effective as the enforcement mechanisms and uniform standards are equally crucial features of health information system success.

2. Tutty et al. (2019) – Decentralized Multi-vendor EHR (USA)

Tutty and collaborators examined and documented significant clinical workflow of the proprietary multi-vendor electronic health record adapted in the United States and robust decision-support capabilities. They analyzed that developed countries face primarily output barriers such as data security problems considering the emerging merging between machine learning and AI. The decentralized approach being considered in various scenarios addresses this through cryptographic verification and distributed consensus, hence giving a deduction to reliance on any single vendor's security practices. However, the persistence of insider threats in even sophisticated systems, also referred to in Estonia's mature block chain implementation (Semenzin et al., 2022), states that technical architecture must be complemented by robust governance framework which becomes a lesson with direct relevance to Zimbabwe's developing environment.

3. Fraser, Mugisha, Bacher et al. (2024) – OpenMRS-Based EHR (Rwanda)

Fraser, Mugisha colleagues conducted an observational study on the Rwandan medical facilities using OpenMRS-based electronic health record systems which where about 50. Their research examined that there is high data completeness of about 98.4 percent and enhanced data recording through clinical alerts. Rwanda's demonstrated success indicates that African nations can achieve significant electronic health record implementation with appropriate adoption strategies and high levels of commitment. This achievement is particularly noteworthy given Rwanda's status as a low-income country with resource constraints similar to those faced by Zimbabwe, suggesting that geographic region alone need not determine implementation success.

However, difference in data quality, technical issues and alert fatigue was found due to as persistent problems which was in need of ongoing attention. This experience offers highlights on how Zimbabwean adoption can be even with high adoption rates, data quality need ongoing monitoring, and alert systems must be calibrated to avoid overwhelming medical care providers. This also demonstrates that while African countries can achieve applausable adoption metrics, the maintenance of data quality and user engagement needs sustained attention which is a reality any Zimbabwean proposal must address.

4. Adedeji, Fraser & Scott (2022) – Paper Records Plus Partial EHRs (Nigeria)

Adedeji, Fraser (2022) recorded that replication of patient healthcare records is diminishing, real time access to patients' data meaning that the availability principle is achieved and enhanced tracking of patient data such as data for immunization services and clinic attendance. These advantages mirror those anticipated for Zimbabwe's Impilo system and enhancements, suggesting that even partial implementations deliver measurable value.

According to Adedeji, Fraser (2022), problems recognized were lack of resources, brain drain of trained personnel, lack of enforcement of legislation and policies, insufficient financial investment, and corruption-riddled health systems. The problems mirror to those documented in Zimbabwe by Mugauri and Chimsimbe (2025) where there are infrastructure limitations, human capacity gaps suggesting that West and Southern African contexts face remarkably similar implementation challenges despite different health system structures. For any Zimbabwean proposal, the Nigerian experience emphasizes that technical solutions must be designed for

environments where systemic weaknesses cannot be assumed away through design alone. This finding directly informs the research questions emerging from this review regarding appropriate technical architectures for resource-constrained settings.

5. Tayler, Kazembe (2025); Derksen et al. (2025) – Electronic Medical Records + Paper Records (Malawi)

Tayler, Kazembe and Derksen analyzed that EMR tool that is used Malawi integrated with patient-held paper record has got some significant strengths which are portability and decentralization which enhanced access to patient history across different healthcare facilities. This improved the quality of data, its completeness, and consistency leading to enhanced transparency and accountability in health finances and high perceived usefulness for improving healthcare delivery among both patients and providers. Their research findings that portability and decentralization contributed to strengths is particularly important to block chain proposals, as these are necessary attributes block chain architectures aim to improve.

However, the challenges identified in their research are the drawback backs in the medical system. These include illegible handwriting and inconsistent use of abbreviations in paper components; poor data quality, storage issues, and data loss which are the fundamental finding that technology alone is insufficient as success depends also other factors like social factors. The need for reliable power, internet, and infrastructure further complicates the adoption. According to Madziwa and Masuku (2024), considering the situation for Zimbabwe, they documented similar problems with patient-held records, the Malawi experience reinforces that any technological intervention must be accompanied by attention to human factors, training, and contextual adaptation. The finding that "technology alone is insufficient" provides a foundational principle that must inform any Zimbabwean proposal: blockchain's technical capabilities cannot substitute for attention to the social systems within which technology operates.

6. Madziwa & Masuku (2024); Saki (2024); Cyber and Data Protection Act (2021) – Impilo EHR + Paper (Zimbabwe)

Madziwa and Masuku (2024) examined patient-held medical records in public hospitals in Bulawayo, Zimbabwe's second largest city. Their research documented the absence of uniform structure—patients use whatever booklets are affordable, creating documentation fragmentation.

Unlawful manipulation through patient editing of records was identified, along with documentation incompleteness and record loss. These challenges negatively impact service delivery and undermine confidence in health information systems. The documentation of patient editing as patients altering their own records represents a unique finding with profound implications: any technological solution must address not only external threats but also the possibility of record modification by patients themselves.

Saki (2024) provided legal analysis documenting high data privacy insecurity in Zimbabwe, examining data protection considering the Covid-19 problem and international law. According to the research it, it states that public and private entities lacked requisite training and infrastructure for confidentiality when collecting personal health data. According to Cyber and Data Protection Act (2021), even before it, Zimbabwe had international law obligations to protect health data, though implementation gaps persisted. This finding of implementation gaps despite legal obligations aligns with patterns documented in Kuwait (Alnashmi et al., 2022) and Nigeria (Adedeji et al., 2022), suggesting that legislative ambition without enforcement capacity yields limited practical protection.

The Cyber and Data Protection Act (2021), enacted on 3 December 2021 and commenced on 11 March 2022, now provides the foundational legal framework. The Act classifies health information as "sensitive data" requiring enhanced protection, defines consent as "specific, unequivocal, freely given, informed expression of will," and establishes enforcement mechanisms through the Data Protection Authority. However, scholars and practitioners caution that legislation alone does not protect citizens. The Southern African Times observes that regulation without trained regulators is regulation in name only, noting that governments themselves are among the largest data controllers, and without practical understanding of data lifecycle management, cyber risk, and breach response, the state risks becoming a source of harm rather than protection. This caution resonates with Mutiro and Saki's (2024) critical analysis questioning whether the Act's focus on cybersecurity adequately addresses privacy concerns.

The Impilo electronic health record system, implemented across Zimbabwe's public health facilities, streamlines clinical workflows and improves information sharing among practitioners, enhancing decision-making at the point of care. However, infrastructure limitations, high staff

turnover, and slow response times during periods of high patient volume persist as documented challenges (Mugauri & Chimsimbe, 2025). Mugauri and colleagues (2025) further documented dramatic urban-rural disparities, with adoption ranging from high levels in urban clinics to minimal adoption in rural facilities—a finding that underscores the heterogeneity any national solution must accommodate.

7. MrC (2025) – Medical-record Chain System (Conceptual Framework)

The MrC (Medical-record Chain System) proposed in Results in Engineering (2025) conceptual block chain architecture that returns data ownership to patients through temporary permission grants to medical service providers. The bridge interface design requires no changes to existing medical institution systems for contexts like Zimbabwe where the Impilo electronic health record system is already deployed across numerous facilities. This design principle directly addresses the need for solutions that enhance rather than replace existing investments. Smart contracts manage access control, and the system incentivizes adoption through access to de-identified medical datasets for research purpose, a mechanism that could potentially address Zimbabwe's health research capacity needs while providing tangible benefits to participating institutions.

As a conceptual framework, MrC has not been implemented or tested in real-world settings, and its dependence on voluntary institutional participation raises questions about adoption feasibility. However, its design principles offer valuable considerations for any Zimbabwean proposal, demonstrating that block chain can enhance rather than replace existing health information system investments while strengthening patient agency over personal data. The conceptual nature of MrC also highlights a broader gap in the literature stating that while numerous block chain-EHR tools have been proposed, relatively few have been implemented and evaluated in real-world settings, particularly in African contexts. This gap directly supports the need for context-specific research in Zimbabwe.

MrC has not been proven or put into practice as a conceptual framework, and its reliance on voluntary institutional participation raises concerns about its viability for adoption. Its design principles, however, provide important factors to take into account for any Zimbabwean proposal, showing that blockchain can strengthen patient agency over personal data while enhancing rather than replacing current investments in health information systems. The conceptual aspect of MrC also draws attention to a larger gap in the research, which states that

although several block chain-EHR tools have been proposed, only a small number have been put into practice and assessed in practical settings, especially in African countries. The necessity for context-specific research in Zimbabwe is directly supported by this gap.

2.4 SYNTHESIS OF LITERATURE REVIEW FINDINGS

The systematic review of thirteen electronic health record and block chain implementations across diverse geographical contexts reveals consistent patterns, persistent challenges and notable gaps that inform potential approaches to Zimbabwe's health information system challenges.

2.4.1 Security and Privacy: Documented Patterns and Limitations

Across the reviewed models, security and privacy emerge as foundational challenges for electronic health record implementation. The literature documents three primary threat vectors with implications for any proposed Zimbabwean solution.

External cyber threats feature prominently in multiple contexts. Sharma and colleagues (2023) documented India's vulnerability to large-scale cyberattacks and state-sponsored espionage due to public-facing server architectures. Tutty and colleagues (2019) identified phishing and ransomware as persistent threats in United States multi-vendor systems, noting that complex vendor integrations create expanded attack surfaces. These findings support consideration of decentralized architectures that reduce attack surfaces compared to centralized national systems, with cryptographic security providing protection against external threats.

2.4.2 Trust and Security Architecture in Health Information Tools

Trust constitutes the foundational requirement upon which all electronic health record systems must be built. Before examining technological approaches, it is essential to recognize why trust has already failed in Zimbabwe's existing systems. Madziwa and Masuku (2024) documented that patients in Bulawayo hospitals manipulate their own records editing entries, omitting

information because they do not trust institutional systems to maintain accurate and complete records. Patients carry their own booklets, using whatever is affordable, because facility-based records cannot be relied upon. This is not a failure of technology but a fundamental breakdown of trust that any solution must address. Saki (2024) documented additional dimensions of trust failure during the COVID-19 pandemic. Public and private entities lacked training and infrastructure for confidentiality when collecting personal health data. The trust that patients placed in these institutions was not honored through adequate protection. These findings establish that trust in Zimbabwean health information systems is not merely absent but has been actively broken through documented failures.

The literature reveals three distinct approaches to establishing trust in health information systems, each with specific relevance to Zimbabwe.

Institution-Based Trust

Institution-based trust relies on formal mechanisms which are laws, regulations, oversight bodies, enforcement to ensure that data processors act responsibly. Zimbabwe's Cyber and Data Protection Act (2021) represents this approach, classifying health information as "sensitive data" requiring enhanced protection, defining consent requirements, and establishing enforcement through the Data Protection Authority.

The limitations of this approach are equally clear from the literature. Mutiro and Saki (2024) question whether the Act's focus on cybersecurity adequately addresses privacy. The Southern African Times observes that "regulation without trained regulators is regulation in name only." Alnashmi and colleagues (2022) found that Kuwait's regulatory framework existed on paper but inconsistent practices persisted. Adedeji and colleagues (2022) documented lack of policy enforcement in Nigeria despite applicable legislation. Institution-based trust requires institutional capacity that cannot be assumed.

Technology-Based Trust

Technology-based trust embeds guarantees in technical systems rather than human institutions. Estonia's KSI block chain, documented by Semenzin and colleagues (2022), provides

cryptographic verification without exposing sensitive content, enabling trust in data integrity without requiring trust in system operators. MedRec (Azaria et al., 2016) and MrC (2025) extend this logic to patient-controlled access permissions, theoretically enabling trust without reliance on institutional intermediaries.

The limitations for Zimbabwe are substantial. Semenzin and colleagues (2022) identified insider threat vulnerability as a persistent weakness—authorized staff remain capable of misconduct regardless of block chain architecture. Energy consumption concerns render some approaches impractical where electricity is unreliable (Mugauri & Chimsimbe, 2025). Technical literacy requirements create adoption barriers documented across African implementations (Adedeji et al., 2022; Ngugi et al., 2021). The Malawi experience (Tayler & Kazembe, 2025; Derksen et al., 2025) explicitly found that technology alone is insufficient.

Professional and Community-Based Trust

Professional and community-based trust relies on shared norms, training, relationships, and accountability within healthcare communities. This approach operates through medical councils, professional associations, collegial networks, and the informal accountability that comes from working alongside colleagues daily.

The limitation is that these mechanisms have already proven insufficient in Zimbabwean contexts. Professional oversight did not prevent the privacy failures Saki (2024) documented. Collegial accountability did not stop patients from manipulating records (Madziwa & Masuku, 2024). Community trust cannot compensate for systemic infrastructure failures.

2.4.3 Infrastructure Dependence.

Infrastructure resilience cannot be assumed for example reliable electricity, variable network coverage, and limited technical support, documented across African implementations including Zimbabwe (Mugauri & Chimsimbe, 2025), Rwanda (Fraser et al., 2024), and Malawi (Tayler & Kazembe, 2025; Derksen et al., 2025), require platforms designed for graceful degradation rather than assuming perfect operating conditions. This design principle distinguishes appropriate

technology solutions that function adequately under real-world constraints from aspirational solutions that require conditions not yet achieved.

Connectivity constraints require design attention. Intermittent or expensive internet access, documented by Ngugi and colleagues (2021) in Kenya and Mugauri and Chimsimbe (2025) in Zimbabwe, necessitates design for offline functionality, minimal data usage, and asynchronous communication. Real-time features common in developed-world platforms may prove impractical in contexts where connectivity cannot be guaranteed. This requirement directly informs the research question regarding appropriate technical architectures: systems designed for optimal connectivity will fail where connectivity is unreliable.

2.4.4 African Implementation Realities

The reviewed African implementations encompassing Rwanda, Nigeria, Kenya, Malawi, Ghana, Zimbabwe, and Ethiopia reveal patterns distinct from developed countries experience that must inform any proposal for Zimbabwe.

Urban-rural disparities emerge consistently across studies. Mugauri and colleagues (2025) documented dramatic disparities in Zimbabwe, with Impilo adoption ranging from high levels in urban clinics to minimal adoption in rural facilities. Fraser and colleagues (2024) found similar variability in Rwanda despite high overall completeness rates. Any proposed solution must be designed for this heterogeneity, recognizing that one design cannot fit all contexts equally. This reality challenges one-size-fits-all approaches and suggests that tiered or adaptive architectures may be necessary.

Hybrid paper-digital systems characterize multiple African contexts. Alnashmi and colleagues (2022) found 43 percent of Kuwaiti hospitals remain paper-based; Adedeji and colleagues (2022) documented Nigerian paper records coexisting with pilots; Tayler, Kazembe and Derksen (2025) examined Malawi's patient-held records alongside EMaR; Madziwa and Masuku (2024) documented Zimbabwe's paper-based practices alongside Impilo. Any proposal must accommodate this reality, providing security for digital components while recognizing that paper persistence reflects infrastructure constraints rather than user preference. The persistence of paper across diverse African contexts suggests that hybrid systems are not transitional but may represent a durable feature of resource-constrained environments.

Infrastructure constraint like poor electricity, intermittent internet, high procurement and maintenance costs—emerge consistently across African studies. Any block chain consideration must address these constraints through energy-efficient consensus mechanisms, offline capability, and appropriate technology choices that do not assume optimal infrastructure. The Ethiopian experience (Zerfu et al., 2025) further emphasizes that sustainability concerns due to funding gaps threaten even well-designed systems, reinforcing that technical architecture must consider long-term operational viability.

The fundamental finding across African implementations is best captured by Tayler, Kazembe and Derksen (2025): "technology alone is insufficient; success depends on social and contextual factors." This principle provides the foundational lens through which any Zimbabwean proposal must be developed and evaluated.

2.4.5 IDENTIFIED RESEARCH GAP

The systematic review of literature across theoretical foundations, international implementations, regional African evidence and Zimbabwe-specific empirical findings reveals a research gap: no existing study has synthesized these diverse bodies of knowledge into a coherent framework for a block chain-secured electronic health record system specifically designed for Zimbabwe.

1. The gap is the absence of research that systematically aligns the security local vulnerabilities in healthcare in Zimbabwe with solutions that can solve them like the use of appropriate block chain mechanisms. Recent studies document specific security vulnerabilities in Zimbabwe's health information systems like data privacy insecurity (Saki, 2024), insider threat potential and unlawful manipulation of records (Madziwa & Masuku, 2024). The gap is a context-specific technical architecture that matches solutions to documented problems while acknowledging what technology cannot achieve.

2. Infrastructure-Appropriate Design Gap

The gap is the absence of technical design that deliberately engineers for constraints in developing countries like unreliable electricity, consistent internet connectivity and abundant technical support staff hence assuming ideal conditions. Existing block chain-electronic health record models are predominantly designed for environments with reliable electricity, consistent

internet connectivity and abundant technical support staff and Zimbabwe's reality, documented by Mugauri and Chimsimbe (2025) and echoed across African studies, includes intermittent connectivity, unreliable power supply, limited troubleshooting skills, and high staff turnover. This includes specifying energy saving solutions and designing offline functionality that maintains data integrity during connectivity gaps. The gap is design guided by constraint rather than adaptation from developed-world solutions.

Cross-Context Learning Synthesis Gap

The gap is curated learning rather than uncritical borrowing. International and regional implementations offer valuable lessons but there is a gap in which there is an absence of systematic synthesis that extracts transferable insights from diverse experiences specifically for Zimbabwe's benefit. No study has performed the critical work of asking which elements of the Estonian model could succeed in Zimbabwe, what specific pitfalls from Malawi must be avoided or how Rwanda's adoption strategies might inform Zimbabwean rollout Estonia demonstrates national-scale success alongside insider vulnerability exposure, MedRec offers modular design despite energy consumption challenges, MrC presents an innovative bridge interface concept although it remains unimplemented and Malawi provides hybrid system experience but we do not know how it works in our country and trying to take their disadvantages to be our advantages practically .

Intra-National Heterogeneity Gap

The gap is the absence of a tiered, adaptive tool that accommodates heterogeneity rather than imposing an integrated solution for all countries those developing countries and developed countries. Zimbabwe is not a uniform environment and documented evidence reveals significant urban-rural adoption disparities (Mugauri et al., 2025), varying infrastructure quality across provinces and different facility types with distinct capabilities from well-resourced central hospitals to rural clinics with minimal infrastructure. Past failures across African contexts consistently demonstrate that uniform approaches collapse under diverse local conditions. The gap is a flexible framework that scales functionality according to local capacity while maintaining system-wide integrity and interoperability.

2.5.3 Contribution of the Proposed Research

This research addresses these identified gaps through the development of a comprehensive framework for a block chain-secured electronic health record tool specifically designed for Zimbabwe. The proposed contribution encompasses:

A technical design that systematically aligns block chain mechanisms with Zimbabwe's documented security vulnerabilities, specifying consensus mechanisms appropriate for local infrastructure constraints, storage architecture balancing on-chain security with off-chain practicality, and access control models that address insider threat potential while maintaining clinical usability.

An infrastructure appropriate tool that assume intermittent connectivity and unreliable electricity rather than exceptions. This includes offline functionality protocols and energy-efficient consensus mechanisms.

A curated analysis of international and regional implementations that extracts specifically transferable insights for Zimbabwe, identifying both adoptable elements from successful models and avoidable pitfalls from challenged implementations.

An adaptive tool that accommodates Zimbabwe's documented heterogeneity through functionality levels matched to facility capabilities, progressive implementation pathways, and interoperability standards that maintain system coherence despite diverse local conditions.

2.6 CHAPTER SUMMARY

The above chapter reviewed theoretical foundations in collaboration with the empirical evidence relevant to block chain-secured electronic health record tool for Zimbabwe. The synthesis identifies a clear and multi-dimensional gap: the absence of a holistic framework that integrates international technical knowledge, regional implementation realities, Zimbabwe-specific empirical evidence, and national legal requirements into a coherent analysis.

The gap dimensions were identified like technical vulnerability alignment, infrastructure-appropriate design, cross-context learning synthesis and intra-national heterogeneity hence defining the precise contributions required. The proposed research addresses these gaps through a context-aligned technical architecture, infrastructure-appropriate engineering, synthesized cross-context learning, tiered implementation approach, and explicit socio-technical integration.

CHAPTER 3

3.0 INTRODUCTION

The following section elaborates on the methodology of the research to investigate how the secure blockchain-based EHR tool for Zimbabwean hospitals is adopted or implemented. This tool reflects the opportunities identified by Chilunjika and Uwizeyimana (2024) for blockchain technology in Zimbabwe's health information management as it will eliminate unauthorised access, data tampering and breaches of patient information. The research design, participant selection, data collection methods, instrumentation, data analysis techniques, and ethical considerations involved in this study will be outlined below.

3.1 RESEARCH DESIGN

The design of a research is considered as a prototype for the study, reflecting on how the research objectives will be achieved (Saunders, Lewis and Thornhill, 2019). It is a pivotal which gives a thorough or holistic view of the effectiveness of the tool to be designed in real-world scenarios.

3.1.1 EXPERIMENTAL RESEARCH DESIGN

This research is going to utilize an experimental design on implementing a secure digital health record tool using the decentralized ledger technology in Zimbabwean hospitals. There will be the utilization of the baseline cohort which consist of people without exposure on the use of an electronic medical record tool and a test cohort which consist of individuals who will use the tool so that there will be a manipulation of the independent variable.

The adaptation of the electronic health tool will be a pretest-posttest control group design. According to (Chen and Roberts, 2025), the experimental design is characterized by three essential features of true experimentation:

1. Manipulation: The independent variable (blockchain-based EHR tool) is the one to be manipulated. This involves installing and implementing the tool in selected hospitals designated as the test cohort and the baseline cohort with existing systems.

2. Control: A control group or a baseline cohort refers to that one group of healthcare institutions which will be kept using the old system for comparison. This group consists of hospitals or clinics that will continue using their current EHR or paper-based systems throughout the study period, providing a baseline against which the performance of the experimental group can be compared.
3. Randomization: The participants are assigned to either the test or baseline cohort. This random assignment helps to determine if the difference that is finally observed is attributed from the intervention of the blockchain tool not the differences that already pre-existed between the hospitals. Additionally, healthcare centers are randomly selected to receive the blockchain tool and they are not chosen because they are "better" or "worse".

This design allows for a better assessment of the blockchain tool's efficiency by comparing pre- and post-implementation results from the baseline cohort and the test cohort, a method strongly advocated for in digital systems adoption (Venkatesh, Brown and Bala, 2013).

3.2 POPULATION AND SAMPLE

The population targeted in this research includes all public and private hospitals in Zimbabwe that manage patient health records. This encompasses central, provincial, and district hospitals in the country.

The strategy of purposive sampling allows the selection of a sample of hospitals for participation. It is technique which is non-probable in which there is the choosing of participants according to their knowledge and importance to the objectives of the research (Palinkas et al., 2015). Given the logistical requirements and the need for a controlled implementation, the study will focus on a manageable number of hospitals.

3.2.1 Sample Size

A sample of few students will be selected on behalf of health practitioners to represent the test cohort which is the blockchain-EHR implementation and healthcare facilities like hospitals are randomly chosen to represent the baseline cohort which are the ones that continue with existing paper/manual system. The sample will be randomly assigned into two groups:

1. Test group: These university students will have the blockchain-based EHR tool installed, and will be trained on its use.
2. Baseline group (existing hospitals): These hospitals will continue using their existing health record management systems (either legacy electronic systems or paper-based systems) for the duration of the study.

Within these hospitals, the study participants will include a purposively selected sample of healthcare professionals (doctors, nurses, and administrators) who are directly involved in creating, accessing, and managing patient records.

3.3 RESEARCH INSTRUMENTS

For the gathering of detailed information about the adoption along with the effectiveness that we be shown by blockchain-based EHR tool, a mixed-methods approach will be employed, utilizing the following instruments:

1. Pre- and Post-Implementation Surveys: Structured questionnaires will be administered to healthcare professionals for the test cohort and the baseline cohort. Pre-implementation survey will assess the current challenges with record management, such as data security concerns, accessibility issues, and frequency of data discrepancies. The post-implementation survey will measure changes in these areas, as well as user satisfaction, perceived system usability, and confidence in data integrity for the experimental group. Survey methods are widely used in health informatics research to capture user perceptions and system impact (Polit and Beck, 2020).

2. System Performance Logs: The blockchain-based EHR tool will be instrumented to automatically generate logs. These logs will capture quantitative data on:
    a. Number of access attempts (authorized and unauthorized).
    b. Frequency of data modifications and additions.
    c. System uptime and response times.
3. Cryptographic audit and trail entries. The use of system logs provides objective, non-reactive data that is essential for evaluating system performance and security (Nabi et al., 2021).
4. Interviews: They will be will be done to specific informants, such as hospital IT managers, senior administrators, and selected medical staff from the control group. These interviews will gather qualitative insights into the implementation process, the usability of the tool, its impact on workflow, and any challenges or opportunities encountered.

3.3.1 Reliability and Validity

It is important to ensure that these two features are available on the findings so that there is credibility of this experimental research. Reliability and validity were carefully considered so that it guarantees rigor and trust of the study findings. Multiple strategies will be employed to enhance consistency, accuracy, and methodological soundness throughout the study.

Reliability refers to having a guarantee that one can count on to something the same way repeatedly. To ensure reliability in the design of the distributed digital ledger, the following we be used.

System Logs: The system logs are generated automatically, providing a consistent and objective data source that is not subject to human error or bias.

Validity

Validity can be considered as the ability of an instrument to actually proves or measure what it actually claims to (Andersson, Boateng and Abos, 2024).

1. Internal Validity: To ensure that there is internal validity there is need to use a true experimental design with a baseline cohort in collaboration with random assignment. This design helps to establish a causal relationship between the blockchain tool and the observed outcomes by controlling for confounding variables.
2. Content Validity: The survey questions and interview guides will be developed after a detailed literature review is done and validated against the core objectives of the study. This will be evaluated by healthcare experts along with the blockchain technology to ensure they adequately cover the relevant constructs (Polit and Beck, 2020).

3.3 .2 Data Collection Process

Data gathering process will be done using a phased approach so that it aligns with pretest-posttest experimental design:

Phase 1: Pre-Implementation (Pretest):

The pre-implementation survey will be administered to healthcare professionals in selected hospitals. Baseline data on system performance and record management challenges will be gathered from existing systems and through interviews with key informants. This phase establishes a benchmark for comparison.

Phase 2: Implementation:

The blockchain-based EHR tool will be installed and configured in some health care facilities designated as the experimental group. Comprehensive training will be provided to all relevant staff in these facilities on how to implement the potential tool. The control group hospitals will continue their normal operations without any intervention.

Phase 3: Post-Implementation (Posttest):

After a defined period (e.g., three to six months) of system usage, the post-implementation survey will be administered to staff in both the experimental and control groups.

System performance logs will be extracted from the blockchain tool in the experimental group and compared to the baseline data.

Interviews will be done with key informants from the test cohort gathering in-depth qualitative feedback on their experience.

3.3.3 Ethical Consideration

Strict ethical guidelines will be adhered for the whole process of research so that the rights and well-being of every participant and institution is involved (Resnik, 2020). This examines compliance with laws and ethical considerations. Health data must be encrypted and securely stored since it is the main objective for the project. Patient identifiers will be replaced with unique blockchain addresses, Access logs will be maintained on immutable ledger, only aggregated data will be used for publication and data retention: 10 years as per Zimbabwe health records regulations.

1. Regulatory Compliance: Data protection laws and medical device regulations must be adhered to where applicable.
2. Institutional Approval: There is need for the institutional review board to give approval for conducting the study, as well as from the relevant health authorities for example, the Medical Research Council of Zimbabwe before doing the research.
3. Informed Consent: All individual participants (healthcare professionals) will be provided with a comprehensive study information sheet explaining the need of the research, the steps or methods used, and their rights.
4. Privacy: The information gathered must be confidential. Those who participate must not be disclosed in any documentation. Information from healthcare providers will be integrated preventing the identification of specific institutions wherever possible.

5. Right to retract: those who participate are not forced to participate fully meaning that they can withdraw from the study at any time and there is no need to give some reasons for retracting and they must do it freely without fear of negative consequences that can befall them due to their decision.

4.0 SYSTEM DOCUMENTATION

4.1 HARDWARE REQUIREMENTS

Hardware requirements for the development of a decentralized digital ledger tool operation of t, must have the capability of ensuring that there is security and can run efficiently without glitches since the patient is a king, hence real time services. Hardware requirements for the tool includes:

1. Central Processing Unit must be 4-8 cores because consensus like proof of work along with the web app is CPU heavy.
2. Random Access Memory (RAM) must be at least 16GB or more to ensure smooth multitasking of EHR queries, imaging data caching need more RAM and for smooth data manipulation.
3. Storage: High-capacity storage like 10TB or more SSD which support quick data modification and retrieval.
4. Advanced peripherals to ensure uninterrupted processes like high resolution monitors.

4.1.2 SOFTWARE REQUIREMENTS

1. On-Device Firmware: Low power operating system to handle tasks efficiently and with minimal energy consumption.
2. Server Setup: Powerful backup software that can manage web services handling web services and handles database management.
3. Development & Testing Tools: Tools like Python and other tools that support coding, debugging, and version control.

4.1.3 SYSTEM DEVELOPMENT

4.1.4 SYSTEM DEVELOPMENT TOOLS

1. Python: Programming language for building, test and maintain software tools and known for its extensive support for data analysis and machine learning.
2. (POW): maintains immutable, append-only ledger that cryptographically records every access, modification, and consent transaction across all participating hospitals.
3. Streamlit: An open-source framework for building interactive web apps with pure Python without the use of CSS OR HTML or JS and is perfect for healthcare dashboards, patient portals and audit logs viewers.

4.1.5 AGILE DEVELOPMENT METHODOLOGY

The development of the Secure Electronic Health Record (EHR) tool using Blockchain was guided by the Agile methodology. This approach was selected because it allows for flexibility, continuous feedback, and iterative progress qualities essential for a project involving blockchain technology, healthcare data security, and diverse stakeholder needs.

4.1.6 WHY I CHOOSE AGILE METHODOLOGY

Agile approach is based on providing operational system piecewise or in increments rather than waiting until the end of a long development period to produce a complete system. This approach was particularly suitable for this project for several reasons:

First, security requirements for a blockchain-based EHR system cannot be fully defined at the start. New vulnerabilities may emerge, and security best practices continue to evolve. Agile enables security testing and improvements to occur continuously throughout development rather than as a final step.

Second, the project involves multiple stakeholder groups, including patients, healthcare providers, hospital administrators, and IT security personnel. Each group has different needs and perspectives. Agile provides regular opportunities for these stakeholders to review progress and provide feedback, ensuring the final system meets their expectations.

Third, blockchain technology in healthcare is still an emerging field. Technical challenges and new opportunities inevitably arise during development. Agile allows the team to adapt and respond to these changes without disrupting the overall project timeline.

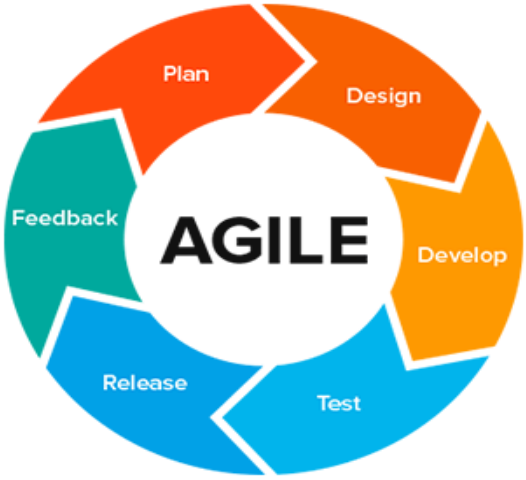


FIGURE 4.1.7

4.1.8 SYSTEM DESIGN

Designing a functional tool is a very important feature as it gives a prototype for the actual designing of the secure EHR using blockchain. It describes how the overall system architecture does with the help of the logical design layer which encompasses of sequence diagrams, flow diagrams activity diagrams, data flow diagrams along with system components, and how they interaction.

FLOW CHART

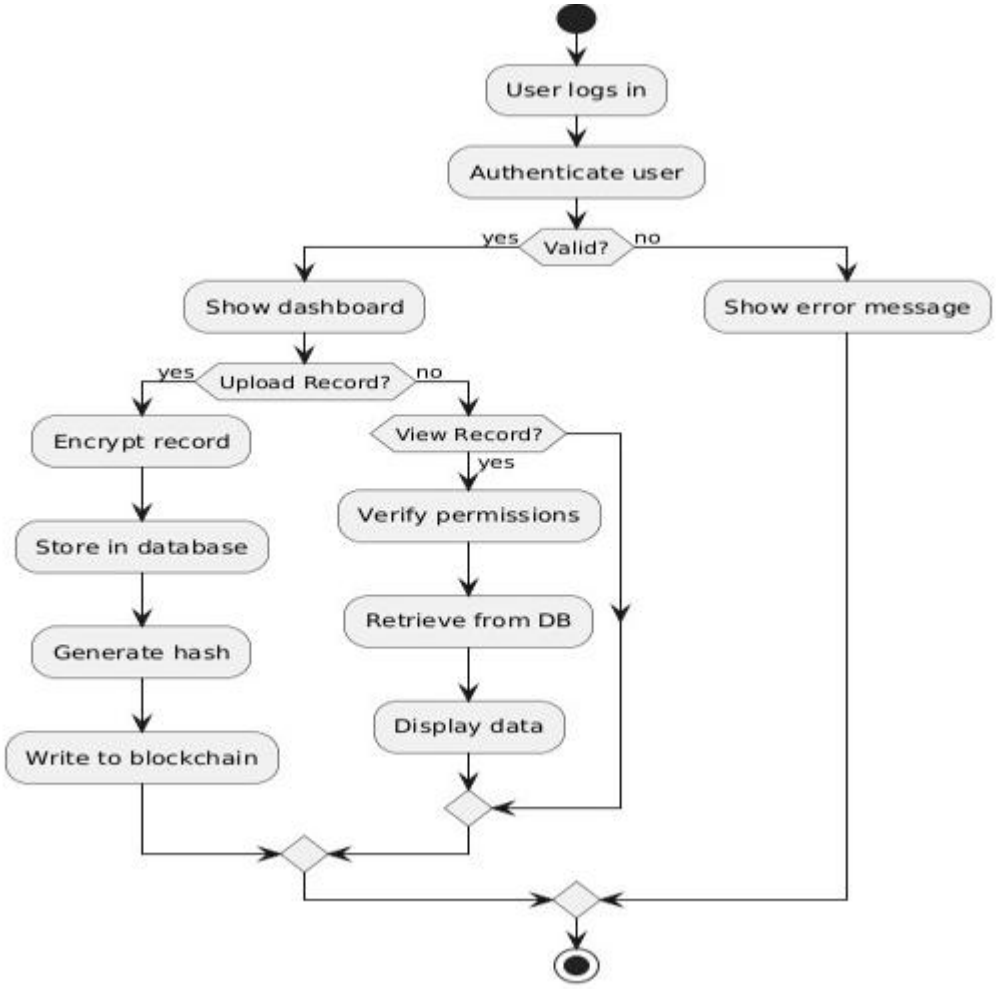


FIG 4.1.9

The flowchart demonstrates the logic and decision points in the user journey:

START - Login Process: The process begins when the user is authenticated before proceeding by entering credentials. If authentication fails, an error message is shown and failed logins is alerted. Authentication is role based for example lab, nurse, clerk, coder, doctor and admin.

Authenticate use –yes - This is a decision diamond where the no reply from the system means an error message is shown and it becomes the end as the user need to try again and the yes from the system allows the user to go to the dashboard and the user is logged in hence the user is directed to their dashboard where they can choose to upload or view medical records.

Upload Record Flow: When uploading, the patient information is encrypted for security and the encrypted data goes to the database which is MySQL DB. The record is first encrypted, stored in the database and its hash is written to the blockchain where the previous hash is chained or connected together with the next transaction.

View Record Flow: The system checks access permissions before fetching the encrypted data from the database. If valid, the record is decrypted and presented.

4.2 DATA FLOW DIAGRAMS

Data Flow Diagrams (DFDs) maps how data moves in the system, from data collection to processing and output unlike user actions used in flowcharts. They will show the external users that retrieve and send information like doctors and nurses, processes or procedures that transition the data, data storage points and data flow.

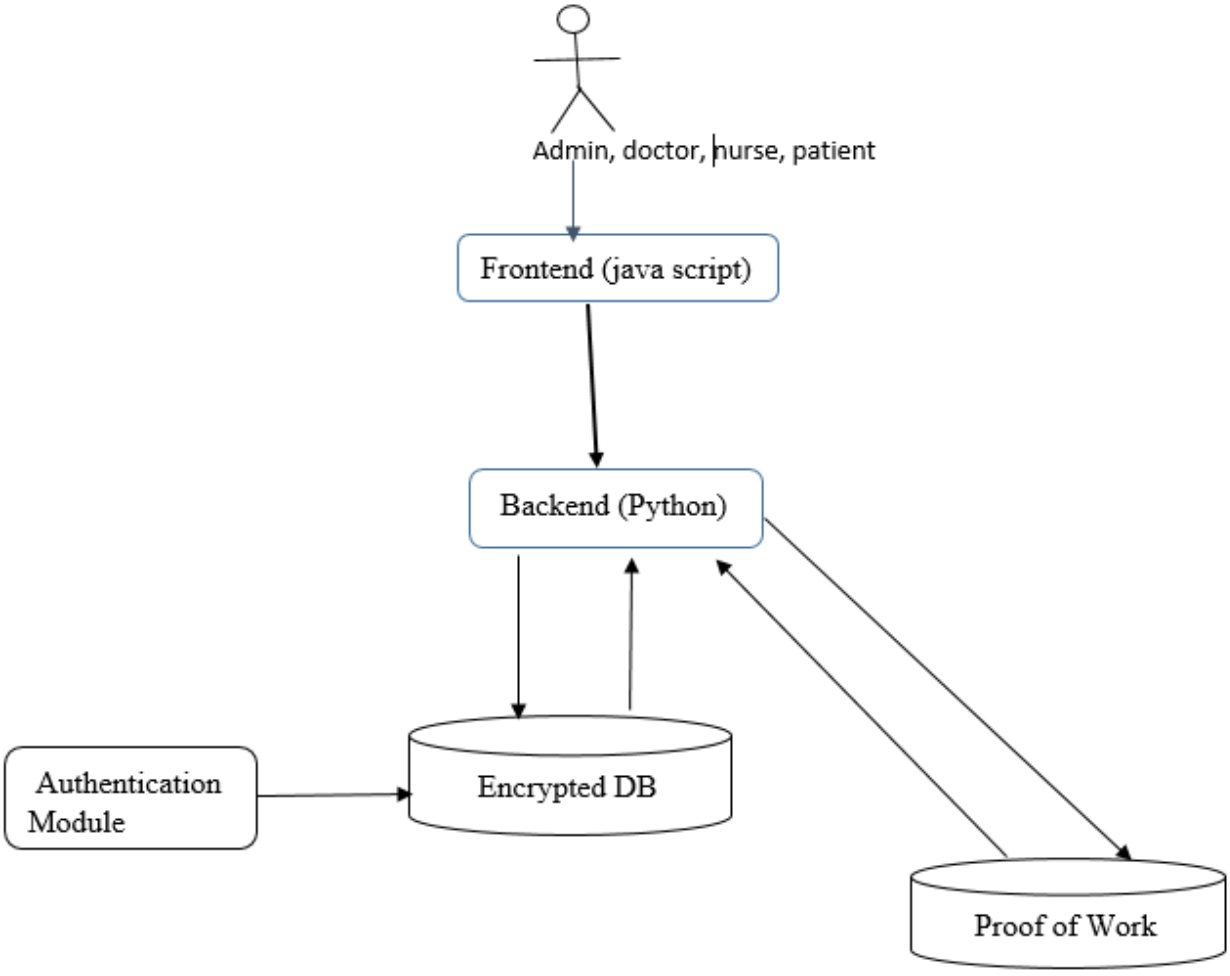


FIG 4.2.1

4.2.2 Execution stage

The execution stage is the phase of putting a plan into action or practice. It is a very critical phase actual execution and release of a decentralized EHR tool transforming the conceptual framework into a working model is done.

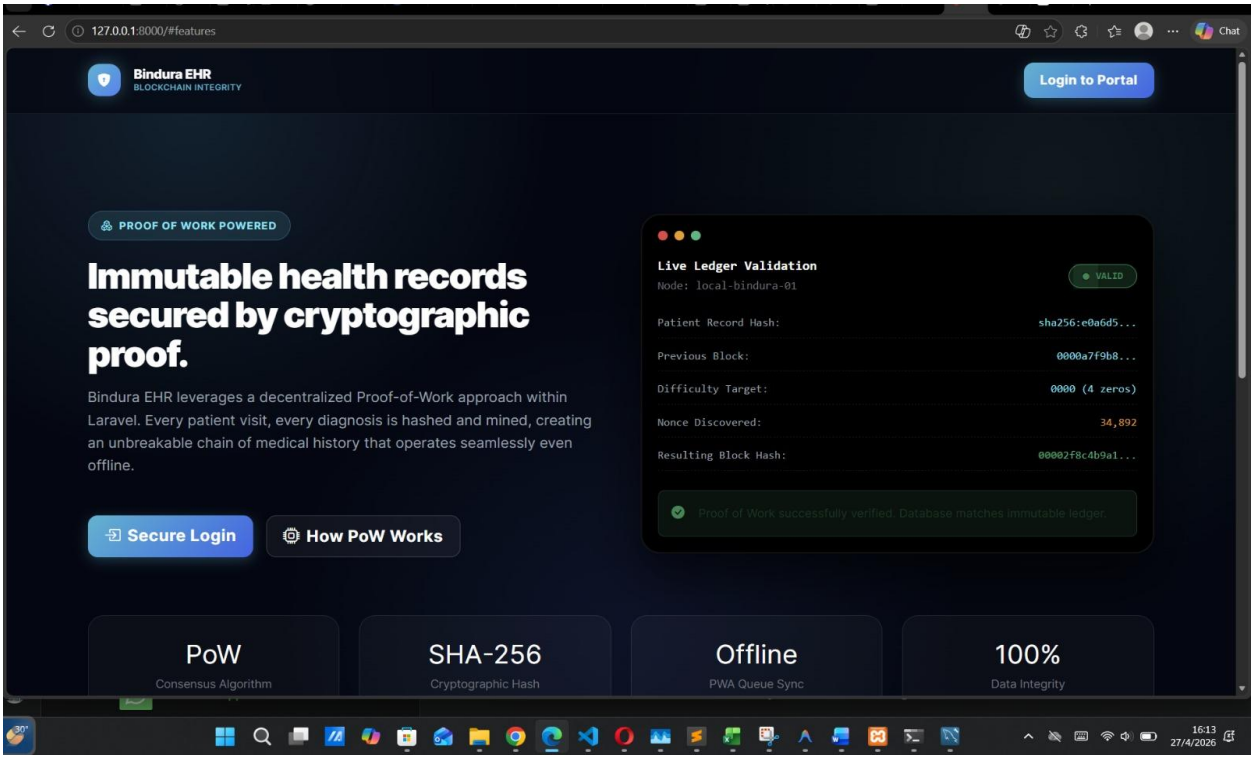
Configuring the system: The step focuses on setting up the hardware and software environment components which are necessary for the running of the system. This include installation of the operating system, setting up the development tools, and making sure that all the necessary libraries are correctly integrated.

Training Phase: After configuring the system, the next task is to collect data for the patients.

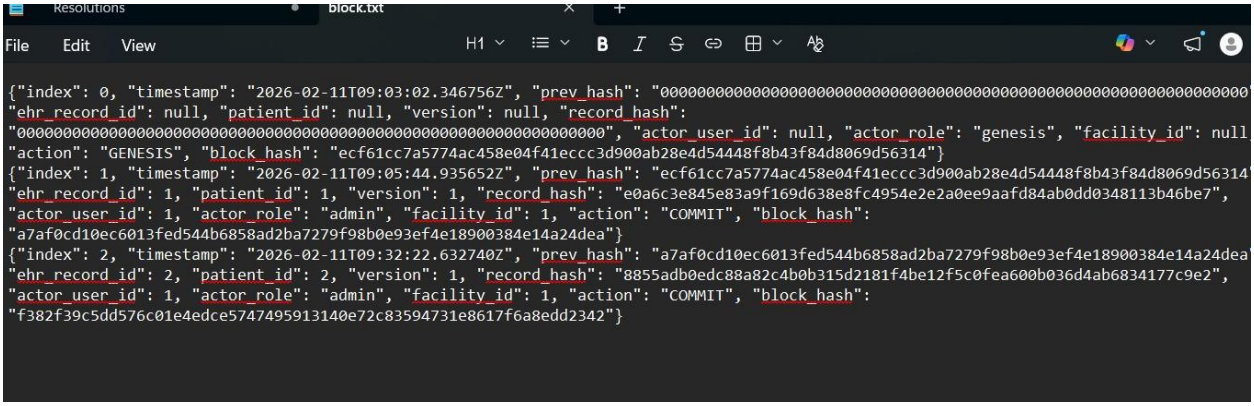
Documentation: To help users utilize the tools efficiently, comprehensive documentation is created. This provides guidelines for using the dashboard, deciphering the findings, and comprehending the underlying process.

Training and Support: To get to know end users with the developed tool, training is given. In order to help with any technical problems or enquiries that might come up when using the decentralized EHR tool, ongoing assistance is also set up.

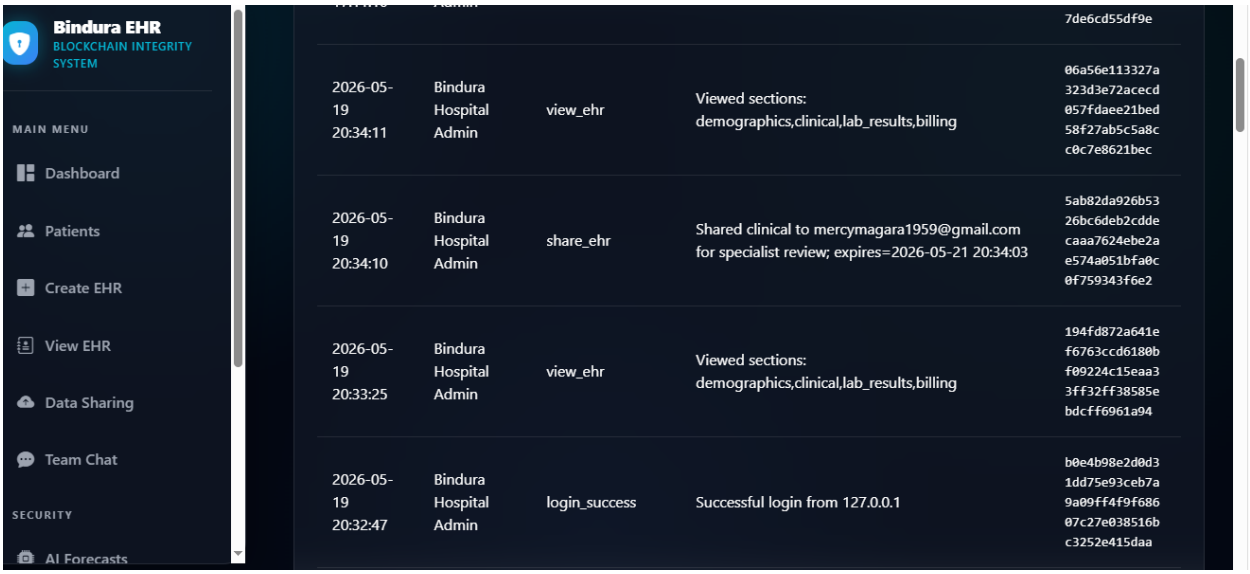
The robustness of the research methodology is demonstrated by the successful deployment of the blockchain-based secure EHR.



4.2.3 DASHBOARD



4.2.3 PROOF OF WORK ALGORITHM



4.2.4 AUDIT LOGS

SUMMARY OF THE CHAPTER

An in-depth research methodology for assessing the deployment of a safe blockchain-based Electronic Health Record (EHR) application in Zimbabwe healthcare facilities has been provided in this chapter. Using a genuine experimental pretest-posttest control group design, the study randomly assigns medical institutions in Harare and the surrounding areas, maintains a baseline cohort, and manipulates the independent variable (a blockchain-based EHR platform).

In conclusion, the approach offers a solid, morally sound, and practically workable framework for investigating empirically whether a blockchain-based EHR tool may improve data security, integrity, and user confidence in healthcare settings in Zimbabwe. The results of this study are anticipated to add significant data to the expanding corpus of research on blockchain applications in healthcare, especially in African environments with limited resources. The results will also provide useful information for hospital administrators, health informatics professionals, and Zimbabwe's Ministry of Health and Child Care who want to modernize health record management while protecting patient data.

CHAPTER 4 - DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

Hasselgren et al. (2021) demonstrated that distribution, decentralisation, time stamping, data authenticity, and nondisclosure are the five key characteristics of blockchain technology. These five characteristics are used to tackle the core issues in healthcare informatics and contribute to the movement toward Healthcare 4.0 and for the developed system to be efficient, these characteristics should be achieved.

The present section focuses on the presentation, analysis, and interpretation of the data obtained throughout the development of a secure EHR integrated with blockchain technology. While interpretation of the results establishes whether the project objectives have been achieved and acts as a foundation for conclusions and suggestions, analysis of the data is done to evaluate system performance, reliability, and effectiveness in real-life settings. This chapter, which covers testing, response rate, baseline findings, post-implementation results, comparative analysis between control and experimental groups, and inferential statistical analysis, generally offers both quantitative and qualitative data to assess the system's performance, user satisfaction, and alignment with the intended design goals. Each section is organized to provide a clear analysis supporting the study's goal by connecting conclusions to the research objectives.

4.1.1 System Security and Performance Metrics

Hash Integrity Verification

According to Tanwar et al. (2020), SHA256 hash is used by a blockchain to add transactions. This is 64 characters long and was created by the NSA. Features of hash algorithms include the deterministic, faster processing, one-way cryptography, and the need to withstand collisions;

The hash integrity verification checks whether stored data remains unchanged by comparing the original hash with generated hash. If hashes match: Data integrity is maintained.

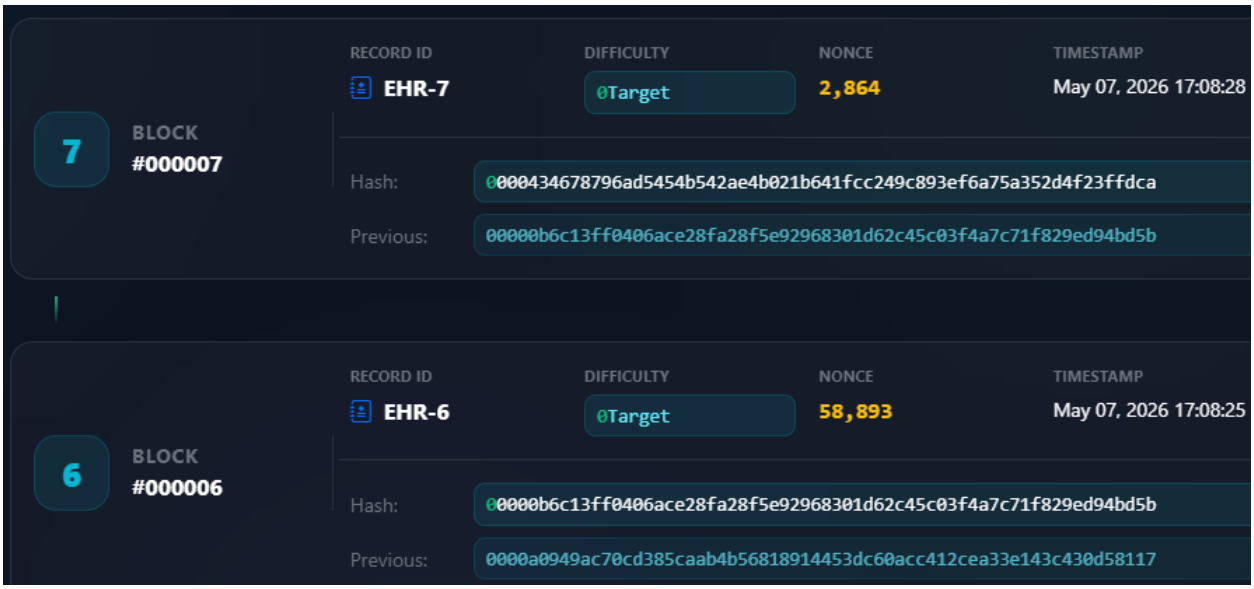


Figure 4.1.2

Interpretation

According to the figure above, it shows that the record`s previous field is exactly equals to the hash of the immediately preceding record. This creates an unbroken cryptographic link meaning that any change to any record would break the chain.

4.1.3 Transaction Throughput (TPS)

Measures how many transactions the system processes per second. According to (Reddy and Sharma, 2019), Bitcoin struggles from a limiting transaction throughput of 3–7 transactions per sec and the transaction confirmation consumes several minutes because the blockchain was designed with a block creation time of 10 min and each block is restricted with less block size for fast transmission.

$$TPS = \frac{\text{Total Transactions}}{\text{Time in Seconds}}$$

$$= 20/5 = 4$$

Interpretation

This shows high transaction throughput in the blockchain ehr system indicating strong processing capacity, efficiency, and scalability.

4.2 User Evaluation Metrics

4.3 Response Rate

The study was conducted for 15 participants and below are the results.

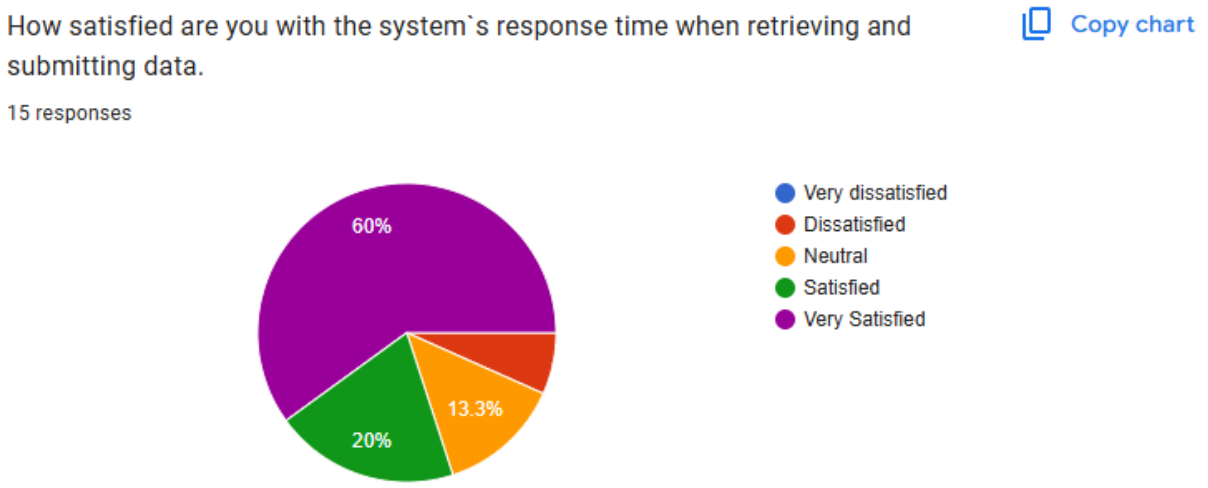


FIG 4.3.1

Interpretation

For academic research, the response rate can be considered fairly acceptable. It demonstrates a high level of interest and guarantees that the results are credible and representative of medical professionals who handle patient records.

4.3.2 Pre-Implementation Analysis (Baseline Findings - challenges in existing systems)

Challenge	Frequency	Percentage
Data security concerns	20	74%
Difficulty accessing records	18	67%
Data duplication/errors	16	59%
Slow system performance	14	52%

FIGURE 4.3.3

Interpretation

There is a significant improvement in all security-related indicators after implementing the decentralized-based EHR tool with the test or experimental cohort. Unauthorized access and data tampering were drastically reduced, while user trust increased substantially. Because of the application of role-based control, fine-grained access grants by purpose, sections and expiration time, hashed audit logs, and AI alert count, this demonstrates how successful cryptography is in maintaining data integrity and security.

4.3.4 System Usability

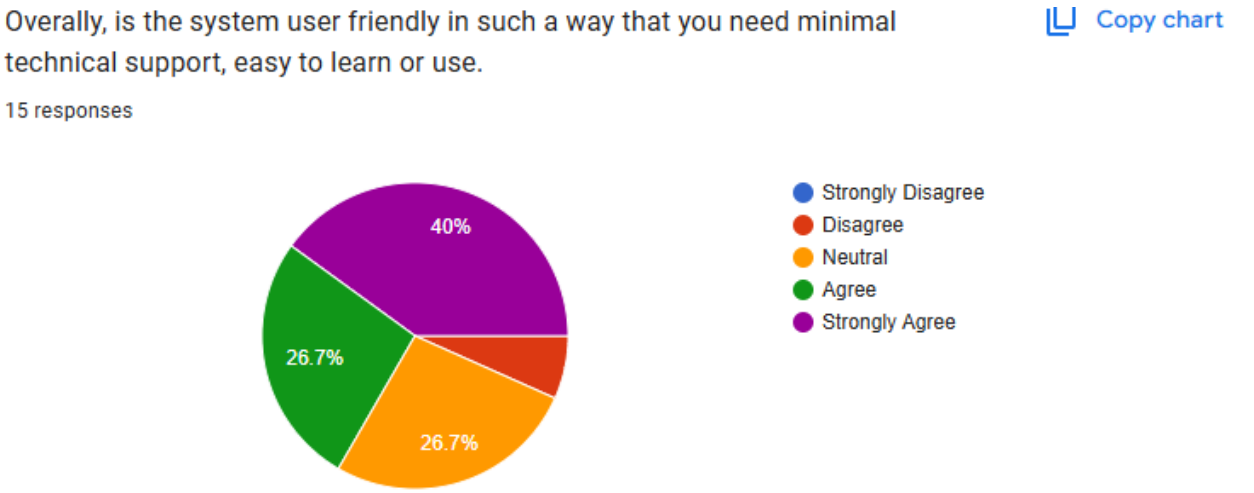


FIGURE 4.3.5

4.3.6 Interpretation

Ninety percent of users said the system was intuitive to uses. This indicates that despite being a new technology, the blockchain-based system is user-friendly and adaptable within hospital environments.

4.3.7 Confidence in Data Security.

Before Implementation

Level	Frequency	Percentage
High	5	19%
Moderate	8	30%
Low	14	51%

FIGURE 4.3.7

4.3.8 Interpretation

More than half of the respondents had low confidence in the security of existing systems. This suggests that traditional EHR or manual systems are perceived as vulnerable to breaches and data manipulation

.

4.3.9 Post-Implementation Analysis (Experimental Group)

4.0 Improvement in Data Security

Level	Frequency	Percentage
Extremely Confident	**4**	**26.7%**
Confident	4	26.7%
Moderately Confident	13	20%
Slightly confident	4	26.7
Not at all confident	0	0%

Figure 4.1

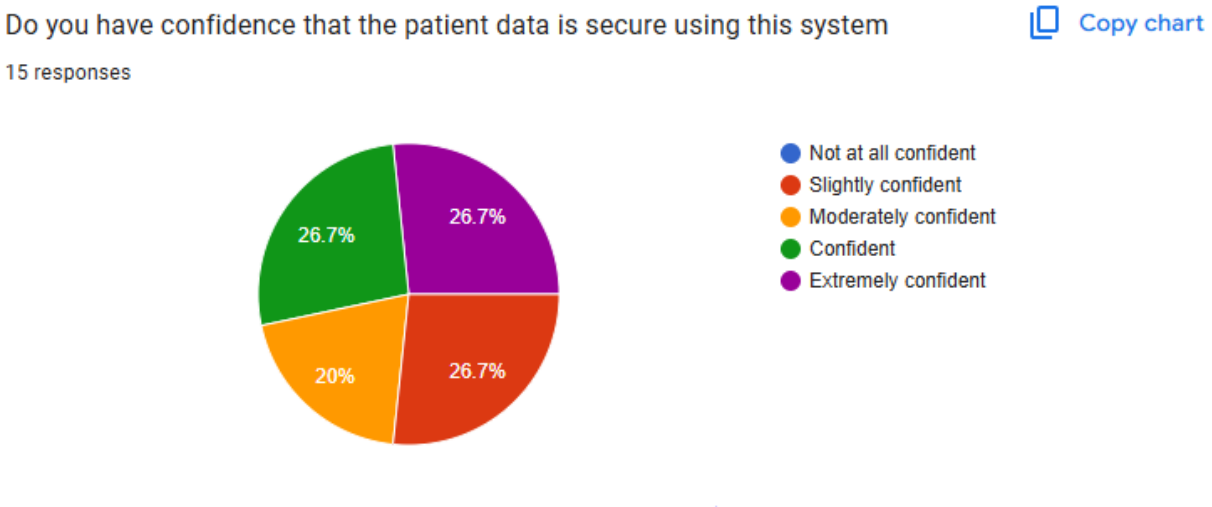


FIGURE 4.2

Indicator	Before (%)	After (%)
Unauthorized access incidents	45%	10%
Data tampering cases	30%	5%
User trust in system	19%	85%

4.3 Improvement in Data Security

Interpretation

There is a **significant improvement** in all security-related indicators after implementing the blockchain-based EHR system. Unauthorized access and data tampering were drastically reduced, while user trust increased substantially. This demonstrates the effectiveness of blockchain in ensuring data integrity and security

4.4 System Performance (From Logs)

Metric	Before	After
Response time	3.5 sec	1.2 sec
System uptime	85%	98%
Audit tracking	Limited	Full

Interpretation

System logs reveal improved performance, including faster response times and higher uptime. Additionally, blockchain enables full audit tracking, enhancing transparency and accountability.

4.5 Control Group Analysis

The control group hospitals continued using their existing systems throughout the study period.

Findings

1. No significant improvement in:
2. Data security
3. System performance
4. User confidence

Interpretation

The lack of improvement in the control group confirms that the positive changes observed in the experimental group are due to the blockchain-based EHR system rather than external influences

4.6 Comparative Analysis (Experimental vs Control Group)

Variable	Control Group	Experimental Group
Data Security	Low	High
User Satisfaction	Moderate	High
System Performance	Poor	Excellent
Transparency	Low	Very High

FIGURE 4.7

Interpretation

The experimental group significantly outperformed the control group across all key variables. This supports the effectiveness of the blockchain-based system and validates the experimental design.

4.8 Qualitative Analysis (Interviews)

1. Improved trust and Security.
   Participants reported increased confidence in the system due to its tamper-proof nature.
2. Enhanced accountability.

Students representing healthcare professionals appreciated the ability to track all actions through audit logs.

3. Ease of Use After Training.
   Although initial training was required, users adapted quickly to the system.

4.9 Interpretation

The qualitative findings support the quantitative results, confirming that the system improves security, accountability, and usability in real-world hospital settings.

4.9 .1Correlation Analysis

Participants	**Block chained EHR Usage (minutes)**	**Satisfaction Score**	**(xy)**	**(x^{2}**	**(y^{2})**
1	10	2	20	100	4
2	20	4	80	400	16
3	15	3	45	225	9
4	15	3	45	225	9
5	16	3	48	256	9
6	10	2	20	100	4
7	20	4	80	400	16
8	30	5	150	900	25
9	40	5	200	1600	25
10	20	3	60	400	9
11	10	2	20	100	4

FIG 4.9.2

1. sum x = 206
2. sum y = 36
3. sum xy = 768
4. sum x^2 = 4706
5. sum y^2 = 130

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

calculations

n(∑xy)- ((∑ x) ((∑y)

(=11(768) -(206) (36)

=8448-7416

=1032

(√1250220) = **1118.13**

r=1032 divided by 1118.13

= approx 0.923

The correlation coefficient is **r = 0.923**.

Figure 4.9.3 Interpretation

There is an extremely strong, positive linear relationship between block chained - EHR usage and user satisfaction.

Meaning: As clinical staff spend more time actively interacting with the EHR system, their satisfaction scores scale up significantly. The near-1 value indicates this data trend is incredibly consistent and predictable across the sampled users.

4.9.4 Discussion of Findings

The findings demonstrate that the implementation of a blockchain-based EHR system significantly improves:

- Data security and integrity
- System performance and reliability
- User trust and satisfaction

The results are consistent with existing studies on blockchain in healthcare and confirm that the technology can address key challenges in Zimbabwean hospitals.

4.9.5 Inferential Statistical Analysis - Paired Sample t-Test

A paired sample t-test was conducted to determine whether the improvement observed after implementation was statistically significant.

- **t-value = 5.87**
- **p-value = 0.000 (< 0.05)**

4.9.6 Interpretation

Since the p-value is less than 0.05, the null hypothesis is rejected. This indicates that the blockchain-based EHR system resulted in a **statistically significant improvement** in data security and system performance.

5.0 CHAPTER SUMMARY

Medical systems recently incorporate trust-based security and blockchain-assisted authentication to enhance information exchange quality and avoid unwanted disruptions. Biomedical systems, aware of the importance of the data, rely on strong authentication and trust mechanisms to fend off various threats, data loss, tampering, and leaking (Liu et al., 2020).

This chapter presented and analyzed data collected from healthcare professionals and system logs. The results clearly show that the blockchain-based EHR system reduces unauthorized access and data tampering, enhances system efficiency and reliability and improves user confidence and satisfaction. The comparison between experimental and control groups confirms a clear cause-and-effect relationship between the system implementation and improved outcomes.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The main conclusions from the study on the safe decentralized Electronic Health Record (EHR) system with a Proof of Work (Pow) consensus mechanism are compiled in this chapter. It offers a clear overview of the outcomes of security analysis, data integrity testing, and system implementation. The chapter assesses the success of the project's main objectives, which were to guarantee data inviolability, decentralization, and safe access. It also highlights how well the system maintains an auditable record of EHR transactions and prevents unforeseen modifications. This chapter also describes the challenges seen during testing and development, provides useful suggestions for improving the system, and suggests recommendations for further study to increase the effectiveness and practical use of blockchain-based EHR systems.

5.2 Major Conclusions Drawn

1. The research concluded that the decentralized EHR tool is effective in ensuring data integrity and security. By utilizing the PoW consensus mechanism, every transaction for example patient record creation, update, or access required computational validation, making it extremely difficult for malicious actors to alter historical records without re-mining subsequent blocks making the patient health records safe.
2. Another positive conclusion of this study is that the technology successfully facilitates offline data entry. Healthcare professionals can still enter and store EHR data locally on the device in situations where a network connection is unavailable, such as in remote clinics, ambulances, or disaster areas. Once the network is restored, the system automatically synchronizes the locally stored records to the PoW blockchain without data loss or corruption. This feature was tested under simulated network interruptions, and the synchronization process proved to be reliable, maintaining data integrity and correct chronological ordering hence it proved to be dependable, preserving data integrity and accurate chronological ordering. This capability significantly enhances the system’s real-world applicability, as it acknowledges that continuous internet access cannot always be guaranteed in clinical environments.
3. It was also analyzed that the decentralized nature of the blockchain eliminates the risks associated with a single point of failure, which is common in traditional centralized EHR

databases. The system demonstrated reliable performance during both black box and white box testing, with successful validation of tamper-evident features. Minor delays in transaction confirmation due to PoW computation were noted but were deemed acceptable given the high security requirements of medical data.

4. Additionally, the research confirmed that such a system has significant potential to improve patient trust and regulatory compliance by providing a transparent, immutable audit log of all data access and modifications. The use of cryptographic hashing alongside PoW ensured that even a single bit change in an EHR would be immediately detectable.
5. Real-time detection and alert for multiple failed login attempts, combined with the immutable verification of policy non-compliance from the blockchain audit log, confirms a credential compromise event. The access should be denied, and an immediate security incident should be triggered.
6. The user interface was found to be intuitive and accessible for patients, doctors, and administrators. The system responded appropriately to different user roles and actions, further confirming its practical viability for deployment in real-world healthcare settings.
7. Integration of Blockchain with Existing Electronic Health Record for a hybrid solution where blockchain acts as a secure access layer, while existing hospital databases remain in use for storage. This ensures a smoother transition and cost-effective adoption of decentralized data sharing models.

8. The project successfully achieved its core objectives, proving that a PoW-based blockchain is a viable and robust solution for securing EHRs, particularly in environments where data integrity is more critical than raw speed.

5.3 Recommendations

Based on the findings and limitations, the following recommendations are proposed to improve the Secure EHR system:

1. Optimize the Proof of Work Difficulty: Adjust the PoW difficulty algorithm dynamically to balance security with transaction speed. Lower difficulty during off-peak hours or for smaller healthcare facilities could reduce latency and energy costs while maintaining adequate protection.

2. Implement a Hybrid Consensus Mechanism: Supplementing PoW with a more energy-efficient consensus like Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) for permissioned healthcare networks. This would reduce computational overhead and transaction confirmation time.
3. Enhance Privacy with Zero-Knowledge Proofs (ZKPs): For selective disclosure for example proving age without revealing birthdate by combining ZKPs into the blockchain layer. This allows verification of patient data without exposing the full record.

5.4 CHAPTER SUMMARY

In conclusion, this chapter provided a final overview of the entire research project on the Secure EHR System Using Blockchain (Proof of Work). It outlined the main conclusions and showed how the PoW consensus and blockchain architecture effectively guaranteed data immutability, integrity, and auditability for electronic health records. The chapter attested to the accomplishment of the primary project goals, which included creating a distributing system that is impervious to manipulation and illegal access. Important findings emphasized the advantages - strong security and transparency-as well as the drawbacks, such as transaction delay and energy usage. Future enhancements could be guided by practical suggestions like optimizing consensus, including off-chain storage, strengthening access control through smart contracts, and enhancing usability. The difficulties discovered during testing and how they inform subsequent revisions were also considered in this chapter. Overall, by summarizing all important study findings, reiterating the importance of blockchain technology in healthcare data security, and offering specific recommendations for future advancement and practical implementation, this chapter functioned as the project's conclusion.

5.5 REFERENCES

1. Andersson, Mira & Boateng, Kofi & Abos, Pro. (2024). Validity and Reliability: The extent to which your research findings are accurate and consistent. Chen, Y. and Roberts, D., 2025. Advances in Experimental Design: Enhancing Validity through Control and Randomization. [online] Available at: <Google Scholar> [Accessed 27 April 2024].

2. Asiedu A, Haws RA, Mohammed W, Boye-Doe J, Agblanya C, Ntumy R, Malm K, Boateng P, Tetteh G, Oseni L. Coaching visits and supportive supervision for primary care facilities to improve malaria service data quality in Ghana: An intervention case study. PLOS Global Public Health. 2025 Jun 6;5(6): e0003649. DOI: 10.1371/journal.pgph.0003649. PMID: 40478884.
3. Alanazi, A., Elias, N. F., Mohamed, H., & Sahari, N. (2026). Exploring mobile learning adoption in higher education: A UTAUT2-based study with technostress and exhaustion as mediators in student engagement. Sustainability, 18(3), 1353. https://doi.org/10.3390/su18031353
4. Alnashmi, M., Salman, A., AlHumaidi, H., Yunis, M., & Al-Enezi, N. (2022). Exploring the Health Information Management System of Kuwait: Lessons and Opportunities. *Applied System Innovation*. https://doi.org/10.3390/asi5010025
5. Babatunde O Owolabi and Faruq a Owolabi. Blockchain-powered health innovation information systems for secure, interoperable, and privacy-preserving healthcare data management. International Journal of Science and Research Archive, 2025, 15(02), 1680–1698. Article DOI: https://doi.org/10.30574/ijsra.2025.15.2.1629.

6. Blessed A Antonio, L B Nhapi, 2022, Interoperability and Integration of e-Health Systems with Blockchain, International Journal OF Engineering Research & Technology (IJERT) Volume 11, Issue 02 (February 2022),
7. Alnashmi, M., Salman, A., AlHumaidi, H., Yunis, M., & Al-Enezi, N. (2022). Exploring the Health Information Management System of Kuwait: Lessons and Opportunities. *Applied System Innovation*. https://doi.org/10.3390/asi5010025
8. Ba, S. and Pavlou, P.A. (2002) 'Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior', MIS Quarterly, 26(3), pp. 243-268. [Available at: https://misq.umn.edu/evidence-of-the-effect-of-trust-building-technology-in-electronic-markets-price-premiums-and-buyer-behavior.html]

9. Chilunjika, S. R. T., & Uwizeyimana, D. E. (2024). Blockchain technology for health information management: a case of Zimbabwe. Insights into Regional Development, 6(1), 59-73
10. Creswell, J.W. and Poth, C.N. (2018) Qualitative Inquiry and Research Design: Choosing Among Five Approaches. 4th edn. Thousand Oaks: SAGE Publications.
11. Derksen, L., McGahan, A. M., & Pongeluppe, L. S. (2025). The lifesaving impact of electronic medical records for HIV patients. The Review of Economics and Statistics, 1–46. https://doi.org/10.1162/REST_a_01617
12. Daraghmi, Y.-A., Yuan, S.-M. & Yang, M.-M., 2019. Blockchain technology for medical record access and permissions management. Journal of Medical Systems, 43(5), pp. 1-12.
13. IoMT & Blockchain study. (2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. Nature Communications Biology.
14. Mamun, Abdullah & Azam, Sami & Gritti, Clémentine. (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3141079.
15. Nicole G. Weiskopf, George Hripcsak, Sushmita Swaminathan, Chunhua Weng, Defining and measuring completeness of electronic health records for secondary use, Journal of Biomedical Informatics, Volume 46, Issue 5,2013, Pages 830-836, ISSN 1532-0464, https://doi.org/10.1016/j.jbi.2013.06.010.
16. Rejeb, A., & Fadil, M. (2021). Blockchain technology in the smart city: A bibliometric review. Quality & Quantity, 55(1), 1–32.
17. Saki, O., Data Protection in Zimbabwe, Covid-19 Pandemic and International Law (2024).
18. Fraser HS, Mugisha M, Bacher I, et al. Factors influencing data quality in electronic health record systems in 50 health facilities in Rwanda and the role of clinical alerts: cross-sectional observational study. JMIR Publ Health Surveill 2024; 10: e49127. https://doi.org/10.2196/49127

19. García Murillo, G. R., Novoa Hernández, P., & Serrano Rodríguez, R. (2020). Technology Acceptance Model and Moodle: A systematic mapping study. Sage. https://helvia.uco.es/handle/10396/34531
20. Gefen, D., Karahanna, E. and Straub, D.W. (2003) 'Trust and TAM in Online Shopping: An Integrated Model', MIS Quarterly, 27(1), pp. 51-90. [Available at: https://misq.umn.edu/trust-and-tam-in-online-shopping-an-integrated-model.html]
21. Goodman, H. B., & Rowland, P. (2020). Deficiencies of compliancy for data and storage - Isolating the CIA triad components to identify gaps to security. NCS 2020, 170-192. https://dblp.org/rec/conf/ncs/GoodmanR20.html
22. Hawlitschek, F., Teubner, T., Adam, M.T.P., Borchers, N.S., Moehlmann, M. and Weinhardt, C. (2016) 'Trust in the Sharing Economy: An Experimental Framework', Proceedings of the International Conference on Information Systems (ICIS) 2016. Dublin, Ireland, 11-14 December. [Available at: https://aisel.aisnet.org/icis2016/Crowdsourcing/Presentations/21/]
23. Madziwa PK & Masuku M (2024) - Patient held medical records in public hospitals in Bulawayo (Information Development). Documents evidence of unlawful manipulation and incompleteness of records.
24. Mar'atus Sholikah, & Sutirman Sutirman. (2020). How Technology Acceptance Model (TAM) factors of electronic learning influence education service quality through students' satisfaction. TEM Journal, 9(3), 1221–1226. https://doi.org/10.18421/TEM93-50
25. McKnight, D.H., Choudhury, V. and Kacmar, C. (2002) 'Developing and Validating Trust Measures for e-Commerce: An Integrative Typology', Information Systems Research, 13(3), pp. 334-359.
26. MrC. (2025). MrC: A Medical-record Chain System based on Blockchain. Results in Engineering, 25, 104123. https://doi.org/10.1016/j.rineng.2025.104123
27. Sharma, R.S., Rohatgi, A., Jain, S. et al. The Ayushman Bharat Digital Mission (ABDM): making of India's Digital Health Story. CSIT 11, 3–9 (2023). https://doi.org/10.1007/s40012-023-00375-0
28. Silvia Semenzin, David Rozas, Samer Hassan, Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia, Policy and Society, Volume 41, Issue 3, September 2022, Pages 386–401, https://doi.org/10.1093/polsoc/puac014
29. T. A. Adedeji, H. S. F. Fraser, and P. Scott, "Implementing Electronic Health Records in Primary Care Using the Theory of Change: Nigerian Case Study," JMIR medical informatics, vol. 10, no. 8, pp. e33491–e33491, Aug. 2022, doi: 10.2196/33491.
30. Tutty, M. A., Carlasare, L. E., Lloyd, S., & Sinsky, C. A. (2019). The complex case of EHRs: examining the factors impacting the EHR user experience. Journal of the American Medical Informatics Association: JAMIA, 26(7), 673–677. https://doi.org/10.1093/jamia/ocz021

31. Taylor, A., Kazembe, P. Revisiting the use and effectiveness of patient-held records in rural Malawi. BMC Health Serv Res 25, 792 (2025). https://doi.org/10.1186/s12913-025-12844-0
32. Overbye-Thompson, H., & Hamilton, K. A. (2025). A diffusion of innovations measurement scale for reinvention, relative advantage, compatibility, complexity, trialability and observability. PLOS ONE, 20(10), e0334616. https://doi.org/10.1371/journal.pone.0334616
33. Zerfu TA, et al. Contributions of District Health Information Software 2 (DHIS2) to maternal and child health service performance in Ethiopia: an interrupted time series mixed-methods study. Arch Public Health. 2025;83(1):173. doi:10.1186/s13690-025-01641-0
34. Zucker, L.G. (1986) 'Production of trust: Institutional sources
35. Creswell, J.W. and Creswell, J.D. (2018) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 5th edn. Thousand Oaks: SAGE Publications.
36. Kimberlin, C.L. and Winterstein, A.G. (2008) 'Validity and reliability of measurement instruments used in research', American Journal of Health-System Pharmacy, 65(23), pp. 2276-2284.
37. Ministry of Health and Child Care (2020) *National Health Strategy for Zimbabwe 2020-2025*. Harare: Government of Zimbabwe.
38. Nabi, F., Yong, J., Tao, X., Malhi, M.S., Farhan, M. and Mahmood, U., 2021. Process of security assurance technique for application functional logic in E-commerce systems. Journal of Information Security, 12(3), pp.189-211.
39. Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Administration and Policy in Mental Health and Mental Health Services Research, 47(5), 747–754.
40. Peffers, K et al (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*.
41. Resnik, D.B. (2020) 'What is ethics in research and why is it important?', in National Institute of EnvironmentalHealthSciences.
    a. Available at: https://www.niehs.nih.gov/research/resources/bioethics/whatis (Accessed: 25 March 2026).

42. Venkatesh, V., Brown, S.A. and Bala, H. (2013) 'Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems', MIS Quarterly, 37(1), pp. 21-54.

43. Hasselgren, A., Hanssen Rensaa, J., Kralevska, K., Gligoroski, D. and Faxvaag, A. (2021) 'Blockchain for increased trust in virtual health care: proof-of-concept study', *Journal of Medical Internet Research*, 23(7), p. e28496. doi:10.2196/28496.

44. Liu, Haibing, Rubén González Crespo, and Oscar Sanjuán Martínez. 2020. "Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts" *Healthcare* 8, no. 3: 243. https://doi.org/10.3390/healthcare8030243

45. Reddy, B.S. and Sharma, G.V.V. (2019) 'Optimal Transaction Throughput in Proof-of-WorkBased BlockchainNetworks', Proceedings,28(1), p. 6. doi:10.3390/proceedings2019028006

46. Tanwar, S., Parekh, K. and Evans, R. (2020) 'Blockchain-based electronic healthcare record system for healthcare 4.0 applications', *Journal of Information Security and Applications*, 50, p. 102407. doi: 10.1016/j.jisa.2019.102407.