HEALTHCHAIN NIGERIA: A BLOCKCHAIN-BASED SYSTEM FOR SECURE AND INTEROPERABLE HEALTHCARE RECORDS

BY

MBOSOWO GOODNEWS STEPHEN

PSC2105356

DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF COMPUTING,

UNIVERSITY OF BENIN

BENIN CITY, EDO STATE

NOVEMBER, 2025

HEALTHCHAIN NIGERIA: A BLOCKCHAIN-BASED SYSTEM FOR SECURE AND INTEROPERABLE HEALTHCARE RECORDS

BY

MBOSOWO GOODNEWS STEPHEN

PSC2105356

A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF COMPUTING, UNIVERSITY OF BENIN, BENIN CITY, IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF A BACHELOR OF SCIENCE (B.Sc.) DEGREE IN COMPUTER SCIENCE

NOVEMBER, 2025

CERTIFICATION

This is to certify that this project titled "Healthchain Nigeria: A Blockchain-Based System for Secure and Interoperable Healthcare Records" was carried out by MBOSOWO **GOODNEWS STEPHEN** with Matriculation number: **PSC2105356** and submitted to the Department of Computer Science, Faculty of Computing, University of Benin, Benin City, under the supervision of **PROF. F. AMADIN**.

________________________ ____________________

MBOSOWO GOODNEWS STEPHEN Date

Student

________________________ ____________________

PROF. F. AMADIN Date

Supervisor

________________________ ____________________

DR. MAXWELL OSAGIE Date

Project Coordinator

________________________ ____________________

DR. ROSEMARY USIOBAIFO Date

Head of Department

APPROVAL PAGE

This project titled "Healthchain Nigeria: A Blockchain-Based System for Secure and Interoperable Healthcare Records" by MBOSOWO GOODNEWS STEPHEN with Matriculation number: **PSC2105356** has been approved as meeting the requirements for the award of Bachelor of Science Degree in the Department of Computer Science, Faculty of Computing, University of Benin, Benin city.

______________________	______________________
PROF. F. AMADIN Supervisor	Date
______________________	______________________
DR. MAXWELL OSAGIE Project Coordinator	Date
______________________	______________________
DR. ROSEMARY USIOBAIFO Head of Department	Date

DEDICATION

This work is dedicated to the Almighty God, the source of life and giver of grace and strength, who, by his mercies and grace, saw to the finishing of this project work, and this milestone in this academic journey.

ACKNOWLEDGEMENTS

My utmost acknowledgement goes to God Almighty for giving me the strength, wisdom and direction throughout my academic journey. I would like to express my gratitude to my project supervisor PROF. F. AMADIN for his consistent guidance towards ensuring the successful completion of this project.

To The dean (Faculty of Computing), Dr. (Mrs.) R. A. Usiobaifo (Head of Department), Prof. (Mrs.) F.A. Egbokhare, Prof. A. A. IMIANVAN, Prof. G. O. Ekuobase, Prof. (Mrs.) A. O. Egwali, Prof. F. I. Amadin, Prof. F. A. U. Imouokhome, Prof. (Mrs.) S. Konyeha, Prof. (Mrs.) V. I. Osubor, Prof. F. O. Chete, Dr. E. Nwelih, Dr. (Mrs.) G. O. Aziken, Mr. E. E. Obasohan, Dr. F. O. Oliha, Dr. (Mrs.) R. O. Osaseri, Dr. C. E. Igodan, and Dr. M. Osagie, Mr. K. O. Otokiti, Mr. I. E. Obayagbona, Miss. L. O. Usiosefe, Mr. J. O. Okhuoya, Mr. G. I. Evbuomwan and the non-teaching staff, for your various roles and support. I acknowledge your contributions with appreciation.

To my beloved parents, Mrs. Augusta Mbosowo and Mr. Ekerette Mbosowo, I owe a debt of gratitude for their sacrifices, love, and prayers. To my siblings—Emmanuel, Esther, Idara, and Enobong Mbosowo—thank you for your unwavering support and encouragement throughout my academic journey.

Finally, I also want to appreciate those who contributed to the success of this project: Kene Jennifer Amarachi, Kamsiriochukwu Arua Joseph, Odunukwe Ebubechukwu Erioluwa. I would also like to thank my family and friends for their support, words of encouragement, and consistent guidance throughout this project.

ABSTRACT

Healthcare data management in Nigeria remains challenged by fragmented record-keeping, poor interoperability, and heightened risks of data manipulation and security breaches. This study presents HealthChain Nigeria, a blockchain-inspired framework designed to deliver secure, tamper-proof, and interoperable medical record management geared toward the Nigerian healthcare ecosystem. The proposed system employs a Node.js backend with AES-256 encryption for file uploads, a simulated blockchain ledger (via JSON) to record consent and transaction hashes, and a simple web-based frontend for patient, clinician and administrator interface. Key implementation features include patient-controlled access rights (grant/revoke consent), encrypted record storage, and auditable transaction logs. Functional testing demonstrated successful workflows for record upload, consent management, and secure data retrieval only when access is granted. The prototype indicates that blockchain principles—immutability, decentralization, and transparency—can be adapted into resource-constrained healthcare settings to enhance trust, streamline workflows, and protect patient data. The findings suggest that HealthChain Nigeria provides a viable pathway toward more inclusive, efficient and secure healthcare record systems in developing country contexts, with potential for full blockchain integration in the future.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Healthcare remains one of the most vital sectors in any nation, as it directly impacts the well-being and productivity of the population. Globally, advancements in digital health have transformed the way medical services are delivered, enabling data-driven decision-making, improved efficiency, and better patient outcomes. One of the most critical components of this transformation is the effective management of healthcare data. Medical records form the foundation for diagnosis, treatment, and follow-up, and their accuracy, accessibility, and security are essential for quality healthcare delivery (World Health Organization, 2021).

In developed countries, electronic health record (EHR) systems have been widely adopted to ensure that patients' data can be accessed seamlessly across different healthcare providers. These systems promote interoperability, improve care coordination, and enhance patient safety by reducing duplication of tests and preventing errors. However, in many developing countries, including Nigeria, the adoption of digital health infrastructure remains low, and where such systems exist, they are often fragmented, insecure, and poorly coordinated (Okpala et al., 2021).

Nigeria's healthcare system faces multiple structural challenges. Patient records are commonly kept in paper form or isolated digital silos, which makes information sharing across hospitals nearly impossible. As a result, patients who move from one hospital to another often have to repeat diagnostic tests or provide medical histories verbally from memory. This fragmentation leads to increased healthcare costs, diagnostic delays, and in many cases, misdiagnosis or treatment errors (Okafor & Chukwu, 2021). Furthermore, the lack of a unified system hinders health research, policymaking, and effective monitoring of healthcare delivery across the country.

Another pressing issue is the prevalence of security breaches and privacy violations in healthcare institutions. Due to inadequate cybersecurity frameworks and weak compliance with data protection standards, sensitive patient information is highly vulnerable. Breaches not only expose personal health data to malicious actors but also compromise public trust in medical institutions. As Adeleke and Adebayo (2022) noted, Nigerian hospitals have increasingly become targets for cyberattacks, with devastating implications for patient confidentiality and organizational credibility.

Fraudulent practices further compound these problems. Fake prescriptions, falsified records, and manipulation of medical data are widespread, eroding trust and weakening institutional efficiency. Centralized medical record systems are particularly prone to such manipulation because they rely on single points of control, making them vulnerable to tampering and corruption (Nwankwo, 2020).

Against this backdrop, blockchain technology has emerged as a promising innovation to address these challenges. Blockchain is a decentralized, immutable, and transparent digital ledger that can securely store and share data across multiple nodes without reliance on a central authority. In healthcare, blockchain can provide tamper-proof records, verified access to medical histories, and interoperability across healthcare providers. Its immutability ensures that once records are created, they cannot be altered, thereby reducing fraud and enhancing trust (Wang et al., 2021).

The relevance of blockchain in Nigeria extends beyond security. Given the country's infrastructural limitations and digital divide, blockchain solutions can be adapted to support low-connectivity environments through the use of technologies such as USSD and QR codes. This makes it possible to extend digital healthcare services to underserved and rural areas, thereby promoting inclusivity and equity in healthcare access (Ogundele, 2020).

The proposed system, HealthChain Nigeria, is designed as a blockchain-based framework to transform healthcare record management in Nigeria. HealthChain aims to provide secure storage, verified access, and seamless interoperability of medical records across hospitals and clinics. By addressing the problems of fragmentation, fraud, and insecurity, HealthChain has the potential to enhance trust, reduce errors, and improve the overall efficiency of Nigeria's healthcare sector.

1.2 Statement of the Problem

The Nigerian healthcare system faces significant challenges in the management of patient data. Records are fragmented and dispersed across multiple institutions, making continuity of care difficult. Patients are often required to repeat diagnostic tests and recount their medical histories, which increases the likelihood of misdiagnosis and delays in treatment (Okafor & Chukwu, 2021).

Moreover, weak cybersecurity measures have led to frequent breaches, exposing sensitive health information and violating patients' rights to privacy (Adeleke & Adebayo, 2022). This erosion of trust discourages patients from fully embracing digital health solutions.

The situation is worsened by limited access to verified patient histories, particularly in rural and underserved regions, where inadequate infrastructure and poor digital adoption create barriers to effective healthcare delivery (Ogundele, 2020). Additionally, fraudulent practices such as falsified prescriptions and manipulated records undermine the credibility of healthcare institutions and compromise patient safety.

Existing centralized health record systems have failed to solve these problems because they are prone to tampering, lack interoperability, and remain inaccessible to many Nigerians. These challenges underscore the urgent need for a secure, interoperable, and tamper-proof healthcare data management system tailored to Nigeria's context.

1.3 Aim of the Study

The aim of this study is to design a blockchain-based system, HealthChain Nigeria, that ensures secure, tamper-proof, and interoperable healthcare records, thereby improving trust, efficiency, and inclusivity in the Nigerian healthcare sector.

1.4 Objectives of the Study

The specific objectives of the study are to:

1. To design a secure health-record system that uses encryption and a tamper-proof ledger to protect patient data.
2. To develop a consent-controlled access mechanism that ensures only authorized healthcare providers can view patient records.
3. To create an interoperable system architecture that supports seamless data exchange across healthcare providers.
4. To implement a prototype (HealthChain Nigeria) that demonstrates secure record upload, consent management, audit logging, and ledger-based traceability.
5. To evaluate the efficiency, security, and practicality of the proposed system in solving Nigeria's healthcare data challenges.

1.5 Significance of the Study

This study has multiple benefits for key stakeholders in the Nigerian health ecosystem. For patients, it offers greater control over personal health information, ensuring that data is both secure and accessible when needed. For healthcare providers, it reduces errors and fraudulent practices by ensuring that medical records and prescriptions can be verified through immutable blockchain technology (Nwankwo, 2020).

For policymakers and regulatory bodies, HealthChain serves as a strategic framework to drive digital health transformation in alignment with global standards. By promoting transparency and accountability, it supports the enforcement of Nigeria's data protection regulations and strengthens institutional trust. For researchers and academics, the study contributes to the growing body of knowledge on blockchain applications in healthcare, particularly in Africa, where such solutions remain underexplored (WHO, 2021).

Ultimately, HealthChain Nigeria has the potential to revolutionize healthcare record management by improving accessibility, enhancing data protection, and ensuring equitable healthcare delivery across both urban and rural communities.

1.6 Scope of the Study

This study focuses on the conceptualization of a blockchain-based framework for healthcare record management in Nigeria. The scope covers secure storage, verified access, fraud prevention, and interoperability of electronic health records. The study does not include other blockchain applications such as pharmaceutical supply chains or insurance claims. Furthermore, it is limited to theoretical design and analysis rather than full-scale system implementation.

1.7 Definition of Terms

Blockchain: A decentralized digital ledger technology that records transactions across multiple computers in a secure, transparent, and immutable manner.

Electronic Health Record (EHR): A digital record of a patient's medical history, diagnoses, and treatments, maintained by healthcare providers.

Interoperability: The ability of healthcare systems to exchange, interpret, and use data seamlessly across different platforms and providers.

Tamper-Proof Records: Records that cannot be altered or deleted once entered into the system, thereby ensuring data integrity and trust.

USSD (Unstructured Supplementary Service Data): A mobile communication protocol that allows services without requiring internet connectivity,

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The purpose of this chapter is to review existing literature on healthcare record management, blockchain technology, and the potential of blockchain-based solutions for secure and interoperable healthcare systems, with a particular focus on the Nigerian context. A strong literature review provides the foundation for understanding the research problem, highlights gaps in existing systems, and demonstrates why the proposed solution—HealthChain Nigeria—is both timely and necessary.

Globally, healthcare systems have undergone significant transformation in how medical records are collected, stored, and shared. Historically, patient data management began with paper-based documentation, later shifting toward Electronic Health Records (EHRs) and other digital health solutions. However, challenges such as poor interoperability, fragmented systems, lack of security, and data breaches have limited the effectiveness of conventional digital health approaches (Adler-Milstein & Jha, 2020).

The emergence of blockchain technology offers new opportunities for rethinking healthcare record management. Its unique properties—immutability, decentralization, transparency, and security—present a disruptive model that may address long-standing issues within the Nigerian healthcare sector, where inefficiencies, duplication of patient records, and weak data governance frameworks persist (Ogunyemi & Adeleke, 2021).

This chapter is structured to provide a comprehensive review of healthcare records and interoperability issues, the evolution of digital health systems, the role of blockchain in healthcare, and existing case studies from both developed and developing countries. The goal is to establish the context for HealthChain Nigeria as a framework that can enhance secure, efficient, and patient-centered healthcare record management.

2.1 Concept of Healthcare Records

Healthcare records are the backbone of modern health systems, serving as the primary means of documenting, communicating, and evaluating patient care. They contain critical information about an individual's medical history, diagnoses, medications, laboratory results, and treatment plans. The effective management of healthcare records is not only vital for patient safety and continuity of care but also for research, policymaking, and healthcare financing (WHO, 2021).

2.1.1 Definition of Healthcare Records

Healthcare records can be defined as the systematic documentation of an individual's medical history and care across time, created by health professionals for the purpose of delivering effective treatment. These records can exist in multiple formats, ranging from paper-based files to sophisticated electronic databases (Raghupathi & Raghupathi, 2014). According to the World Health Organization (2021), health records are indispensable for ensuring clinical quality, providing evidence of care, and enabling data-driven health system planning.

In the Nigerian context, health records are still largely dominated by paper-based documentation, though gradual digitization efforts are being introduced through government and private sector initiatives.

2.1.2 Types of Healthcare Records (Paper-based, EHR, PHR, etc.)

Healthcare records are generally categorized into the following types:

1. Paper-Based Records: Traditional handwritten documentation stored in physical files. While inexpensive and easy to use, they are prone to loss, duplication, and damage.
2. Electronic Health Records (EHRs): Digital versions of patients' medical charts designed to be accessible across healthcare providers. They enhance efficiency and reduce duplication of tests.
3. Personal Health Records (PHRs): Patient-controlled digital health documents that empower individuals to manage and share their health information (Amatayakul, 2017).
4. Hybrid Systems: A mix of paper-based and electronic records, often seen in transitional healthcare systems such as Nigeria's.

The movement toward EHRs and PHRs reflects a growing recognition of the importance of interoperability and patient empowerment in modern healthcare.

2.1.3 Importance of Healthcare Records in Patient Care

Healthcare records serve several crucial functions:

- Continuity of Care: They ensure accurate tracking of patient history, medications, and allergies, enabling safe and consistent treatment.
- Decision Support: Clinicians rely on medical records for evidence-based decision-making and diagnosis.
- Legal and Administrative Value: Health records serve as legal evidence of care and are essential for insurance claims and audits.
- Public Health and Research: Aggregated health records provide valuable data for epidemiological studies and policymaking (Häyrinen et al., 2008).

For Nigeria, improving healthcare record systems is a pressing necessity, given the prevalence of fragmented systems, duplicate patient files, and weak integration across hospitals and clinics.

2.2 Traditional Healthcare Record Management in Nigeria

Nigeria's healthcare record management system has historically relied on manual paper-based documentation. Despite the growing awareness of digital health technologies, most public hospitals and rural clinics continue to operate with physical files that are vulnerable to theft, damage, and inefficiency (Adeleke et al., 2020).

2.2.1 Paper-Based Systems in Nigerian Hospitals

Paper-based systems remain the default in many Nigerian hospitals, where clerks manually record patient demographics, medical histories, and treatment details. These physical files are often stacked in poorly organized record rooms, making retrieval difficult. According to Eze et al. (2019), patient records are frequently misplaced or duplicated, leading to delays in treatment and administrative inefficiency.

2.2.2 Limitations of Traditional Record-Keeping

The reliance on manual systems poses several limitations:

- Vulnerability to Damage or Loss: Paper files can be destroyed by fire, water, or simple mishandling.
- Data Inaccuracy: Illegible handwriting and missing documentation reduce the reliability of paper-based systems.
- Inefficiency: Retrieval of old records is often slow and time-consuming.

- Security Concerns: Unauthorized access to patient files is common due to lack of proper security protocols.

These issues create gaps in continuity of care and undermine confidence in the healthcare system.

2.2.3 Current Efforts Toward Digital Health in Nigeria

In recent years, Nigeria has begun transitioning toward digital health through several initiatives:

- The National Health ICT Strategic Framework (2015–2020): which aimed to promote eHealth solutions in public facilities.
- Private Sector Innovations: such as mHealth applications for maternal health and telemedicine platforms.
- Pilot Electronic Medical Records (EMR) Systems: implemented in select teaching hospitals and urban clinics.

However, these efforts face challenges including poor infrastructure, inconsistent funding, lack of interoperability, and resistance from healthcare professionals (Ogunyemi & Adeleke, 2021).

2.3 Electronic Health Records (EHRs)

2.3.1 Definition and Global Adoption of EHRs

Electronic Health Records (EHRs) refer to digital versions of patients' medical charts designed to be shared across healthcare providers and institutions. Unlike traditional paper-based records, EHRs are structured, interoperable, and capable of integrating various forms of medical data such as laboratory results, imaging, and prescriptions (Hsiao & Hing, 2014).

Globally, the adoption of EHRs has grown significantly over the last two decades. In the United States, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 accelerated the adoption of EHR systems, with over 85% of office-based physicians using some form of EHR by 2017 (Adler-Milstein et al., 2017). In Europe, initiatives like EHR4CR (Electronic Health Records for Clinical Research) have been launched to foster harmonization of health data across countries. Meanwhile, in low- and middle-income countries (LMICs), adoption remains slower, often hindered by infrastructure gaps, cost, and limited technical expertise (Mutale et al., 2020).

2.3.2 Benefits of EHR Systems

The benefits of EHRs are widely recognized in literature:

- Improved Clinical Efficiency: EHRs reduce redundant tests and support faster access to patient data.
- Enhanced Quality of Care: They provide clinicians with comprehensive patient histories, supporting evidence-based decision-making (Goldstein et al., 2017).
- Data for Research and Public Health: Aggregated EHRs allow for large-scale epidemiological studies and inform health policies.
- Patient Empowerment: Many EHR systems integrate patient portals, enabling individuals to view and sometimes contribute to their health information.

2.3.3 Limitations of EHR Systems

Despite these benefits, EHRs face notable limitations:

- Interoperability Issues: Different EHR vendors often use proprietary formats, limiting seamless exchange of data (Mandl et al., 2012).
- Privacy Concerns: Centralized databases can be vulnerable to data breaches and insider misuse.
- High Costs of Implementation: Deployment requires substantial investment in infrastructure, training, and maintenance.
- Clinician Burden: Poorly designed EHRs increase administrative workload, leading to clinician dissatisfaction (Shanafelt et al., 2016).

For Nigeria, these challenges are more pronounced due to weak ICT infrastructure, lack of interoperability frameworks, and fragmented digital health systems.

2.4 Interoperability in Healthcare

2.4.1 Concept of Interoperability

Interoperability in healthcare refers to the ability of different information systems, devices, and applications to access, exchange, and use health data seamlessly across organizational and geographic boundaries. The U.S. Office of the National Coordinator for Health IT (ONC, 2015) defines interoperability as the capacity for information to move securely and meaningfully between stakeholders to improve health outcomes.

2.4.2 Standards for Interoperability (HL7, FHIR, ISO, etc.)

Globally recognized standards for healthcare interoperability include:

- HL7 (Health Level Seven): A widely used framework for data exchange between healthcare applications.

- FHIR (Fast Healthcare Interoperability Resources): An HL7-developed standard that uses modern web technologies for flexible data sharing.
- ISO Standards: The International Organization for Standardization (ISO) has developed standards like ISO/TC 215 for health informatics.
- DICOM: For imaging data interoperability in radiology and diagnostics.

These standards are designed to foster uniformity in healthcare communication and ensure data integrity across platforms.

2.4.3 Interoperability Challenges in Nigeria

In Nigeria, interoperability remains a major obstacle due to:

- Fragmented Systems: Hospitals and clinics often use different record-keeping methods, making integration difficult.
- Lack of Standardization: Few institutions adhere to global interoperability standards like HL7 or FHIR.
- Infrastructure Gaps: Poor internet connectivity and unstable power supply hinder data exchange.
- Policy Weakness: Limited national frameworks to enforce data-sharing protocols across public and private sectors (Ogunyemi & Adeleke, 2021).

These barriers emphasize the need for decentralized, tamper-proof, and scalable technologies such as blockchain to overcome interoperability challenges.

2.5 Data Privacy and Security in Healthcare

2.5.1 Importance of Data Privacy in Health Systems

Healthcare data is highly sensitive, containing personal and medical information that requires strict protection. Ensuring privacy safeguards patient trust, prevents discrimination, and aligns with ethical and legal obligations (Gostin & Halabi, 2019). Without robust data security, patients may be reluctant to share vital information, undermining the quality of care.

2.5.2 Common Threats to Healthcare Data

Healthcare data faces multiple threats:

- Data Breaches: Unauthorized access to health records, often through cyberattacks.
- Insider Attacks: Employees misusing access privileges to alter or steal information.
- Ransomware Attacks: Malicious software encrypting hospital data until ransom is paid.
- Physical Threats: Theft or destruction of servers and hardware in poorly secured facilities.

According to IBM's 2022 Data Breach Report, healthcare remains the most targeted sector for cybercrime globally.

2.5.3 Existing Nigerian Data Protection Regulations (NDPR, NITDA)

Nigeria has made progress in enacting data protection frameworks:

- Nigeria Data Protection Regulation (NDPR, 2019): Overseen by the National Information Technology Development Agency (NITDA), it establishes principles for lawful data processing.
- Cybercrimes (Prohibition, Prevention, etc.) Act, 2015: Addresses cybercrimes affecting personal and organizational data.

- National Health ICT Strategic Framework: Provides guidelines for secure adoption of health ICT solutions.

Despite these efforts, enforcement remains weak, and compliance levels are low among healthcare institutions (Oladipo, 2021).

2.5.4 Gaps in Privacy and Security Frameworks

The Nigerian healthcare sector still faces significant gaps:

- Weak Enforcement: Laws exist but are not consistently implemented.
- Limited Awareness: Healthcare workers often lack training in data protection practices.
- Infrastructure Challenges: Absence of secure servers and encryption protocols.
- No Unified Patient Identifier: Difficulty in securely linking records across institutions.

These shortcomings highlight the necessity for advanced technologies like blockchain, which embed security and privacy by design, offering cryptographic protection, decentralized storage, and immutable records.

2.6 Blockchain Technology

2.6.1 Definition and Characteristics of Blockchain

Blockchain is a distributed ledger technology (DLT) that enables the recording of transactions across multiple nodes in a network in a way that is transparent, secure, and immutable. The concept was introduced by Nakamoto (2008) as the underlying technology behind Bitcoin, but it has since evolved beyond cryptocurrency into a versatile data management infrastructure.

Core characteristics of blockchain include:

- Distributed Ledger: Data is replicated across all participating nodes, eliminating the need for centralized authorities.
- Immutability: Once recorded, data cannot be altered without consensus, preventing tampering.
- Consensus Mechanisms: Algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) ensure trust among untrusted parties.
- Transparency and Traceability: All network participants can view transactions, fostering accountability (Yaga et al., 2019).

2.6.2 Types of Blockchain (Public, Private, Consortium)

Blockchain systems can be categorized into three main types:

1. Public Blockchains: Open, permissionless networks such as Bitcoin and Ethereum, where anyone can join and validate transactions.
2. Private Blockchains: Restricted to specific participants, often used by enterprises for internal data management.
3. Consortium (Hybrid) Blockchains: Managed by a group of organizations, offering a balance between openness and control (Zheng et al., 2017).

In healthcare, consortium blockchains are often preferred due to the need for controlled access among hospitals, insurers, and regulators.

2.6.3 Key Features (Immutability, Decentralization, Transparency, Smart Contracts)

Blockchain introduces several transformative features relevant to health systems:

- Immutability: Prevents unauthorized changes to medical records.
- Decentralization: Reduces reliance on a single authority, ensuring resilience.
- Transparency: Ensures accountability in data handling and record access.
- Smart Contracts: Self-executing agreements that automate processes like insurance claims and consent management (Christidis & Devetsikiotis, 2016).

2.6.4 Blockchain Applications Beyond Healthcare

Beyond healthcare, blockchain has demonstrated success in:

- Supply Chain Management: Tracking goods from production to delivery.
- Finance and Banking: Enabling cross-border payments and fraud prevention.
- Voting Systems: Enhancing transparency and trust in elections.
- Intellectual Property: Protecting copyrights through immutable timestamping.

These applications highlight blockchain's versatility and justify its adaptation to healthcare contexts where trust, security, and interoperability are paramount.

2.7 Blockchain in Healthcare

2.7.1 Use Cases of Blockchain in Healthcare Globally

Several blockchain-based healthcare projects have emerged worldwide:

- MedRec (MIT, USA): A blockchain framework for managing medical records across institutions.
- Guardtime (Estonia): National-level blockchain deployment to secure health data.
- Medicalchain (UK): A blockchain-based platform allowing patients to control access to their health records.

- BurstIQ (USA): Facilitates secure health data exchange for research and personalized care.

These initiatives demonstrate blockchain's capacity to address long-standing healthcare challenges such as fragmented records and lack of patient ownership.

2.7.2 Benefits of Blockchain for Healthcare

Key benefits include:

- Data Security: Cryptographic mechanisms prevent unauthorized access and tampering.
- Interoperability: Blockchain enables seamless integration across disparate EHR systems.
- Patient Control: Patients can grant or revoke access to their medical data.
- Efficiency: Smart contracts reduce administrative overhead in processes like billing and insurance claims (Agbo et al., 2019).

2.7.3 Limitations and Challenges of Blockchain in Healthcare

Despite its potential, blockchain faces obstacles:

- Scalability Issues: Blockchains may struggle with the massive volume of health data.
- Energy Consumption: Proof-of-Work systems are resource-intensive.
- Regulatory Uncertainty: Healthcare regulations often lag behind technological innovation.
- Data Privacy Concerns: While transactions are secure, storing sensitive medical data on-chain raises ethical questions (Roehrs et al., 2019).

2.8 Blockchain-Based Healthcare Systems in Developing Countries

2.8.1 Case Studies from Africa and Asia

In developing countries, blockchain adoption in healthcare is emerging but promising:

- South Africa: Pilot blockchain projects for pharmaceutical supply chain monitoring.
- Kenya: Use of blockchain to track maternal health interventions through mobile platforms.
- India: State-led initiatives using blockchain for telemedicine and health record management.
- Philippines: Blockchain integrated into health insurance to reduce fraud and streamline claims.

These pilots demonstrate blockchain's adaptability to resource-constrained settings, particularly where infrastructure gaps hinder traditional EHR deployment.

2.8.2 Lessons for Nigeria

Nigeria can draw several lessons:

- Leverage Mobile Penetration: Like Kenya, Nigeria can combine blockchain with mobile health technologies.
- Prioritize Supply Chain: Tackling counterfeit drugs, a major Nigerian health challenge, can be addressed through blockchain tracking.
- Incremental Adoption: Start with pilot projects in tertiary hospitals before nationwide rollout.
- Government Involvement: Strong policy support is essential for sustainable blockchain-based systems.

2.9 HealthChain Nigeria: A Proposed Framework

2.9.1 Rationale for a Blockchain-Based Healthcare System in Nigeria

Nigeria faces persistent challenges in healthcare record management, including fragmentation, forgery, inefficiency, and lack of interoperability. HealthChain Nigeria proposes a blockchain-based framework to address these challenges by ensuring secure, transparent, and interoperable health records.

2.9.2 Expected Features of HealthChain Nigeria (security, scalability, patient control, interoperability)

Key features of HealthChain Nigeria would include:

- Security: End-to-end encryption and immutability to protect patient data.
- Scalability: Optimized blockchain design to handle large volumes of health data.
- Patient Control: Empowering patients to manage access rights to their records.
- Interoperability: Integration with existing EHRs through standards such as HL7 and FHIR.

2.9.3 Potential Challenges and Considerations

Challenges to implementation include:

- Infrastructure Limitations: Unreliable electricity and internet connectivity.
- High Cost: Initial investment in blockchain systems may be prohibitive.
- Regulatory Barriers: Absence of blockchain-specific healthcare policies.
- Adoption Resistance: Healthcare workers and institutions may resist change without proper training and incentives.

Nonetheless, these challenges can be mitigated through phased implementation, public-private partnerships, and alignment with global best practices.

2.10 Theoretical and Conceptual Framework

2.10.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), remains one of the most widely applied frameworks for understanding technology adoption. It emphasizes two central constructs: perceived usefulness (PU), which describes the extent to which individuals believe a technology enhances their performance, and perceived ease of use (PEOU), which captures the degree to which individuals believe using the technology will be free of effort (Venkatesh & Davis, 2000). These constructs jointly influence the attitude toward technology use, which then determines behavioral intention and ultimately actual system use.

Recent empirical studies reaffirm the relevance of TAM in healthcare. For example, *Akinboade et al. (2023)* demonstrated that Nigerian healthcare professionals' willingness to adopt digital platforms was significantly shaped by their perception of usefulness and ease of integration into existing workflows. Similarly, *Shiferaw et al. (2021)* found that healthcare workers in Ethiopia were more likely to adopt electronic medical records when they believed the system would improve patient outcomes and reduce administrative burdens. These findings reinforce that even in resource-constrained environments, perceptions of practical utility and usability are decisive factors in adoption.

Applied to HealthChain Nigeria, TAM underscores a critical challenge: while blockchain technology is inherently secure and decentralized, its adoption depends on whether practitioners believe it will genuinely make their work easier and more effective. For instance, clinicians may only embrace blockchain-based records if they see clear benefits such as reduced duplication of tests, faster access to patient histories, and protection against data tampering. Furthermore, if the interface is overly complex or requires extensive training, perceived ease of use will be low, hindering adoption (Whyte et al., 2023). Therefore, TAM highlights that technological sophistication alone cannot drive success; usability and perceived value are equally essential.

2.10.2 Blockchain Adoption Framework

While TAM offers insights at the individual user level, blockchain adoption also depends on institutional and systemic conditions. The Blockchain Adoption Framework (BAF) extends the analysis by considering broader determinants such as technological readiness, organizational preparedness, regulatory clarity, stakeholder collaboration, and cost considerations (Wang et al., 2019). Unlike conventional digital platforms, blockchain requires a network effect, where multiple institutions—hospitals, insurers, regulators, and technology vendors—must collaborate for the system to be effective.

Recent studies confirm the importance of these broader adoption drivers. *Bazel et al. (2025)*, in a multi-country survey of hospitals, found that adoption decisions were significantly influenced by top management support, partner readiness, cost-effectiveness, and data transparency. Interestingly, government pressure negatively influenced adoption, as hospitals perceived regulatory mandates without adequate support as burdensome. Similarly, *Al-Bassam and Hassan (2022)* argue that infrastructural capacity and cross-institutional trust are critical enablers of blockchain adoption in developing countries.

For Nigeria, the Blockchain Adoption Framework is particularly relevant. Most healthcare institutions lack the infrastructural maturity to implement large-scale blockchain systems. Moreover, regulatory clarity remains limited: while Nigeria has a Data Protection Regulation

(NDPR), blockchain-specific policies are still evolving (NITDA, 2022). Without robust organizational readiness, regulatory support, and stakeholder cooperation, even the most technically sound blockchain system will struggle to scale. Thus, BAF situates HealthChain Nigeria within the broader ecosystem of infrastructural, organizational, and policy readiness, complementing the user-focused insights provided by TAM.

2.10.3 Conceptual Model for HealthChain Nigeria

Drawing from both TAM and BAF, this study proposes a conceptual framework for HealthChain Nigeria that integrates individual, institutional, and technological factors into a coherent adoption model. The model consists of three interdependent layers:

1. Technological Layer – At the foundation, blockchain provides the technical infrastructure, offering decentralization, immutability, smart contracts, and enhanced interoperability. This layer guarantees data integrity and trust in record management, which is crucial in Nigeria where forgery and data manipulation remain persistent problems.
2. User Acceptance Layer – Building on TAM, this layer emphasizes that health professionals' and patients' perceptions of usefulness and ease of use will determine actual engagement. A blockchain system that is technically superior but poorly understood or difficult to operate will face low adoption. Therefore, training, intuitive design, and demonstrable benefits are indispensable.
3. Institutional and Regulatory Layer – Anchored in BAF, this layer highlights the importance of organizational readiness, policy alignment, financial sustainability, and cross-stakeholder collaboration. For instance, alignment with NDPR and future blockchain regulations will build institutional trust, while phased pilots can encourage gradual buy-in from skeptical hospitals.

By integrating these three layers, the conceptual framework acknowledges that HealthChain Nigeria's success cannot be explained by technology alone. Adoption will depend equally on individual perceptions, organizational preparedness, and systemic policy support. This holistic model provides a robust foundation for evaluating feasibility and guides the design of a system that balances technical sophistication with social and institutional realities.

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

This chapter presents the system analysis and design of HealthChain Nigeria, a blockchain-inspired healthcare record management system developed to ensure secure, tamper-proof, and interoperable medical records. The analysis begins by examining the deficiencies of existing healthcare record-keeping methods in Nigeria, followed by the motivation and advantages of adopting the proposed system. The design section then provides the architectural overview, data flow, functional modules, and UML diagrams that collectively form the blueprint for implementation discussed in Chapter Four.

3.1 Analysis of the Existing System

In most Nigerian healthcare institutions, patient information is still managed through paper-based systems or fragmented electronic record systems (EMRs).
Each hospital maintains its own database or manual file room with limited integration between facilities.
When patients move from one hospital to another, their medical history is often transferred through physical copies, phone calls, or incomplete referrals.

This traditional approach leads to several challenges:

- Duplication of medical tests and records.
- Time delays in accessing patient histories.
- Data loss due to poor file storage and mismanagement.
- Difficulty in tracking who accessed or modified sensitive information.
- Lack of verifiable integrity — patient files can be tampered with or misplaced.
- No nationwide interoperability or consistent data exchange format.

These gaps demonstrate the urgent need for a trust-centric, interoperable, and secure system such as HealthChain Nigeria.

3.2 Disadvantages of the Existing System

The existing record-keeping methods suffer from both technical and operational disadvantages:

1. Poor Data Security: Paper files and unencrypted digital systems expose patient data to unauthorized access.
2. Inefficiency: Manual record retrieval and data duplication waste valuable clinical time.
3. Lack of Auditability: There is no transparent log to show who accessed or changed a record.
4. Limited Interoperability: Different hospitals use incompatible systems that cannot share or verify data.
5. High Risk of Data Loss: Files are prone to physical damage, theft, or deletion without recovery mechanisms.
6. Lack of Trust: Patients cannot verify whether their medical records are protected or shared appropriately.

These limitations compromise data integrity, confidentiality, and patient trust, which are essential in modern healthcare management.

3.3 Benefits of the Proposed System

The proposed system, HealthChain Nigeria, directly addresses these weaknesses through a blockchain-inspired architecture that emphasizes encryption, consent management, and verifiable audit trails.

Its key benefits include:

1. Enhanced Security: Patient records are encrypted (AES-256) before storage, ensuring confidentiality even in case of unauthorized access.
2. Immutability and Transparency: Every critical action (upload, consent, access) is logged in an append-only ledger (ledger.json), preventing tampering or deletion.
3. Patient-Controlled Consent: Patients can grant or revoke access to their medical data in real-time.
4. Interoperability: REST-based APIs enable integration with other health systems, paving the way for FHIR compliance.
5. Accountability: Audit logs provide a full trace of all transactions, increasing institutional transparency.
6. Operational Efficiency: Digital record management reduces duplication, speeds up access, and supports remote verification.
7. Scalability and Adaptability: Can be expanded into a full blockchain network later or integrated with mobile/USSD access for rural users.

3.4 Analysis of the Proposed System

The proposed system introduces a four-layer architecture tailored to Nigeria's healthcare environment:

a. Client Layer

This includes the patient, provider, and administrator interfaces (HTML web clients). Users can upload, view, or manage medical records through simple forms and buttons that trigger backend APIs.

b. Backend Layer

Implemented using Node.js (Express), it enforces access control, consent validation, encryption, and audit logging.
It handles RESTful API requests like /api/grant-consent, /api/add-record, and /api/records.

c. Off-Chain Storage

Medical files are stored in an encrypted format (uploads/ folder).
Only hashes and metadata are anchored in the blockchain ledger, preserving security while saving space.

d. Blockchain Ledger (Simulated)

A JSON-based ledger (ledger.json) acts as the immutable blockchain record.
It stores event metadata — transaction ID, hash, timestamp, and actor — allowing auditability without revealing patient content.

Together, these components create a secure, trust-driven workflow that aligns with data protection regulations like NDPR and demonstrates how blockchain principles can be localized for Nigeria's healthcare system.

3.5 Design of the Proposed System

This section describes the system design using UML diagrams to illustrate structure and interactions.

3.5.1 System Architecture Diagram

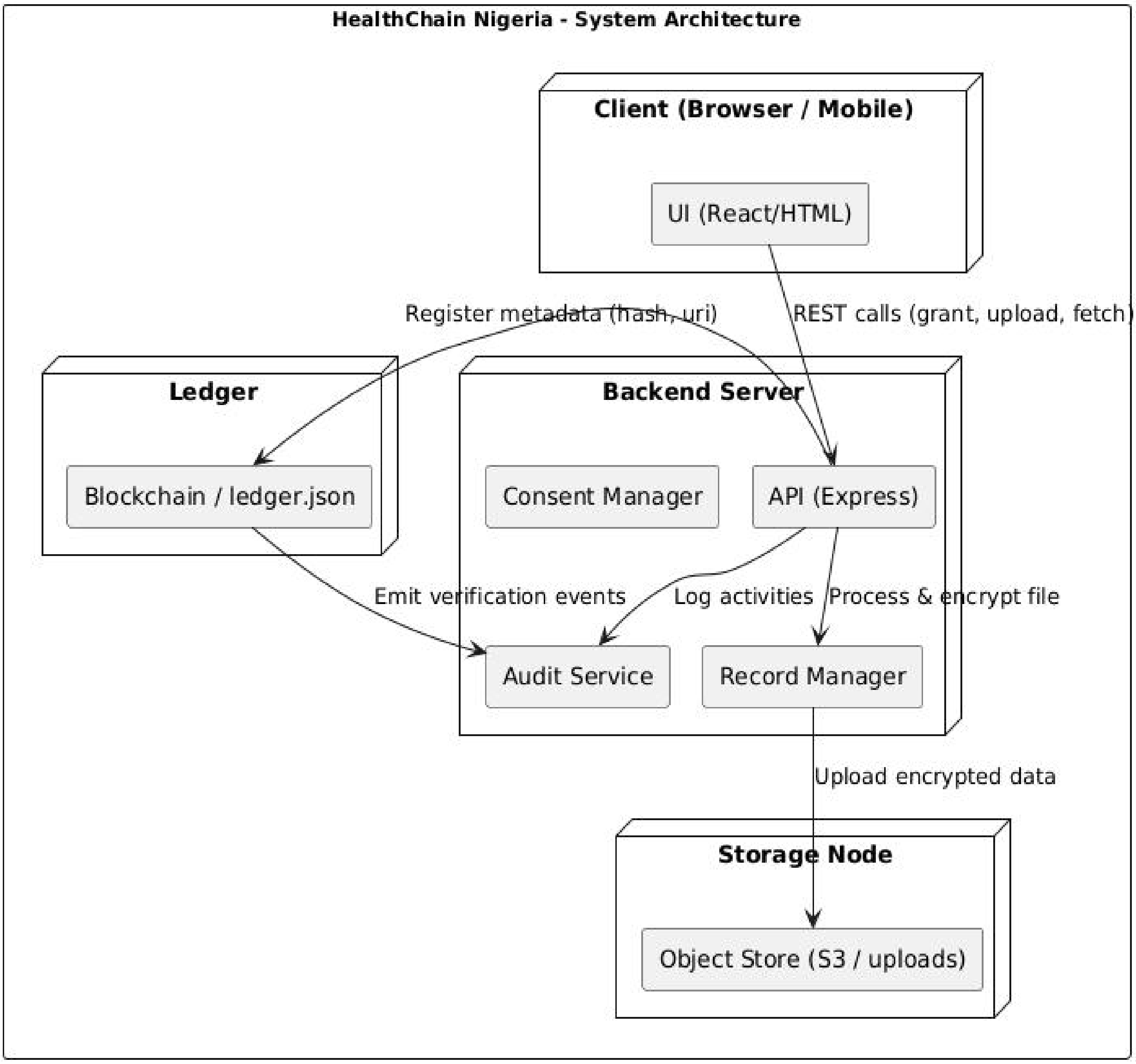

Figure 3.1: *System Architecture of HealthChain Nigeria*

3.5.2 Use Case Diagram

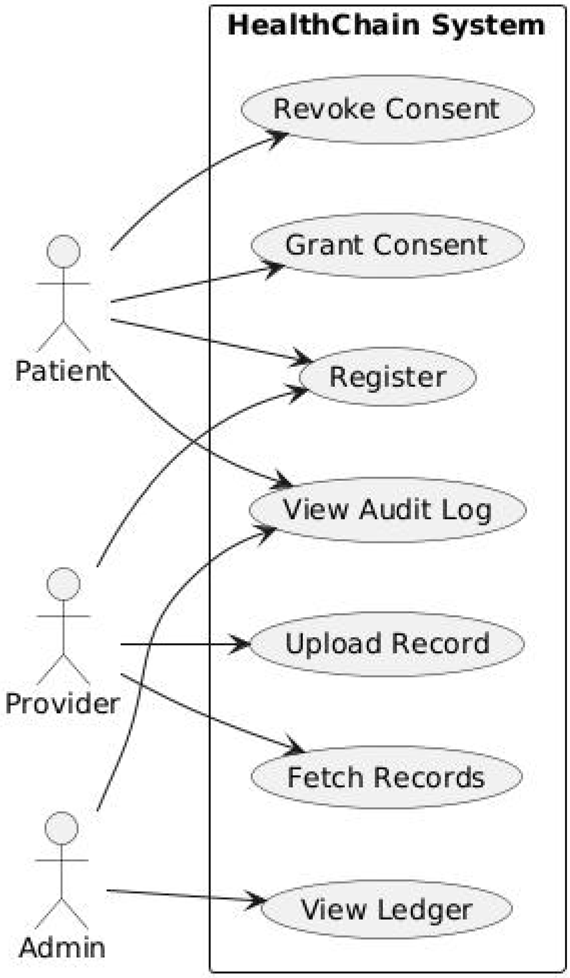

Figure 3.2: *Primary Use Cases of HealthChain Nigeria*

3.5.3 Sequence Diagram – Record Upload Flow

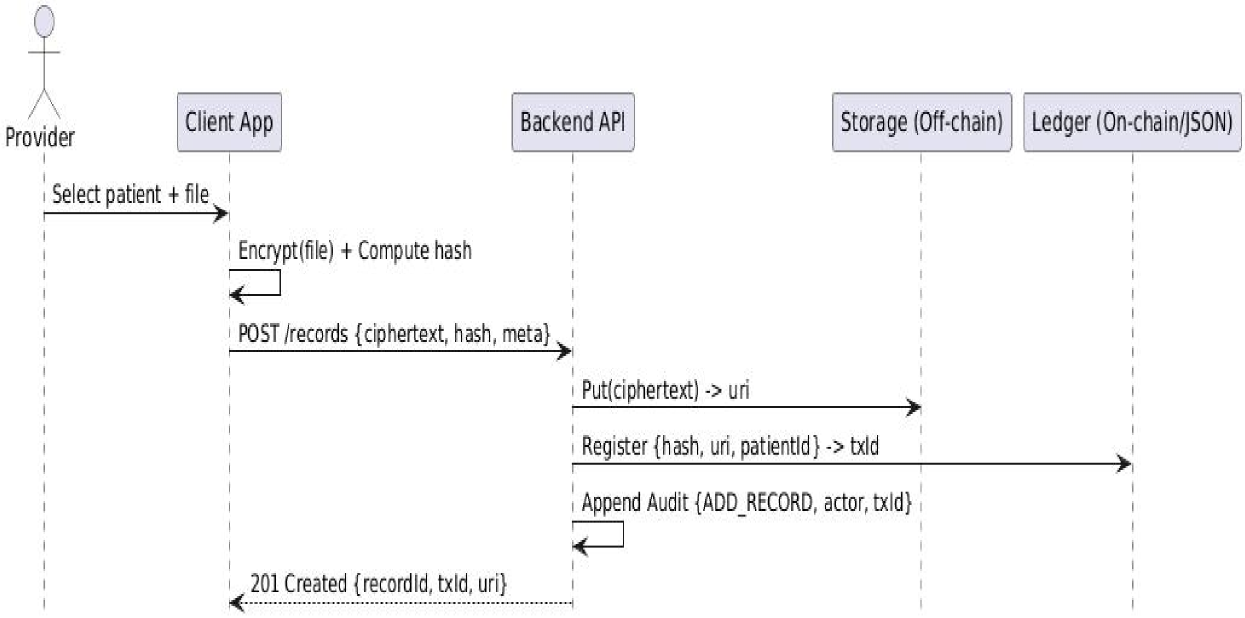

Figure 3.3: *Sequence of Record Upload and Audit Logging*

3.5.4 Consent Granting Diagram

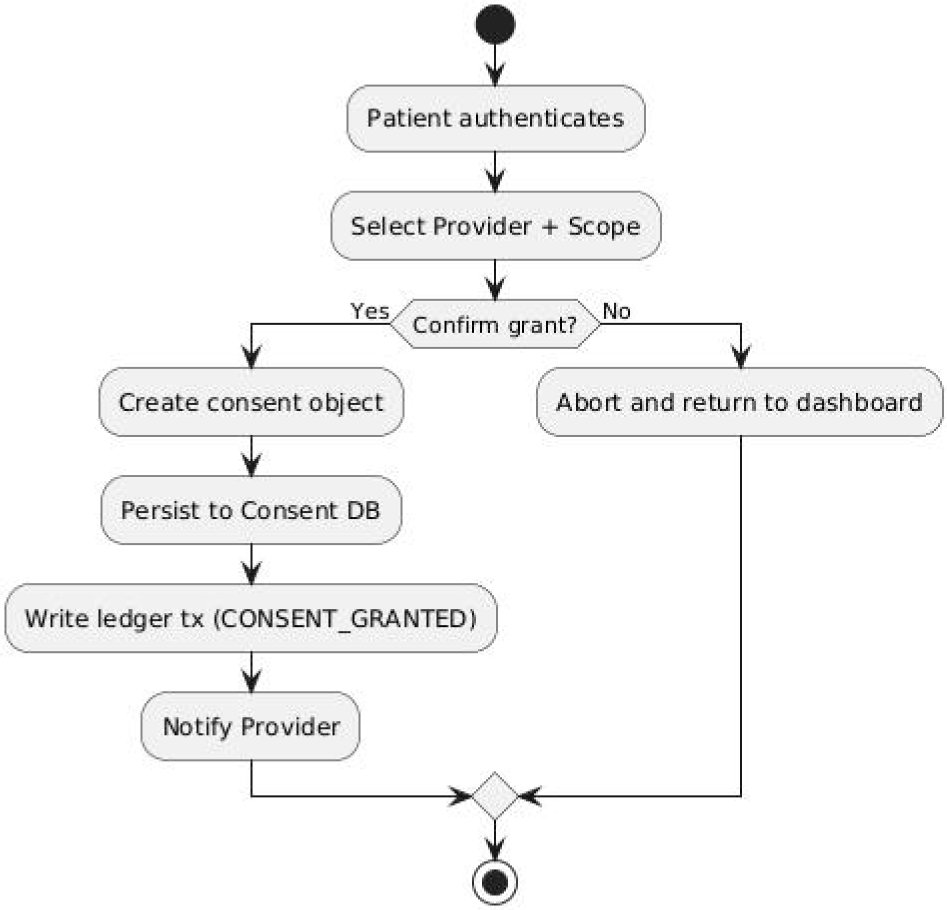

Figure 3.4: *Consent Granting Workflow*

3.5.5 Class Diagram

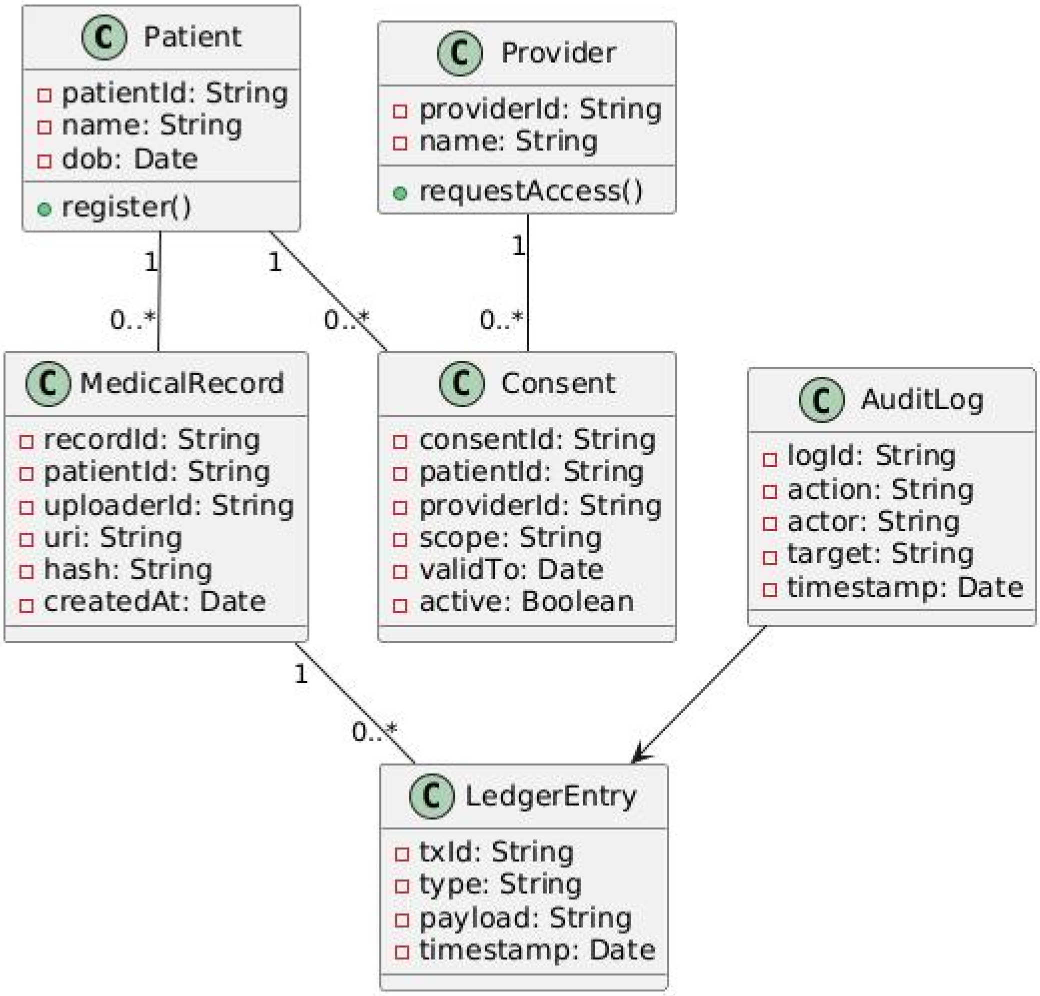

Figure 3.5: *Class Diagram of HealthChain Nigeria*

CHAPTER FOUR

SYSTEM DESIGN, IMPLEMENTATION AND TESTING

4.1 Introduction

This chapter presents the practical realization of the proposed system titled HealthChain Nigeria – A Blockchain-Inspired Healthcare Data Consent Management System. While Chapter Three focused on conceptual modeling and architectural analysis, this chapter translates those models into an operational prototype that demonstrates how blockchain principles—immutability, transparency, and controlled access—can be applied to healthcare record sharing.

The implementation process involved converting the architectural blueprints into executable code using Node.js, Express.js, and a lightweight JSON-based ledger. The prototype integrates secure file encryption, consent-based access, audit logging, and transaction traceability to protect patient information while maintaining ease of use for healthcare providers.

The chapter is organized into six major sections:

- the System Design Overview, which explains how each architectural component interacts;
- System Implementation, detailing the tools, environment, and core modules;
- Testing and Evaluation, verifying the system's performance and reliability;
- Deployment and Maintenance, explaining how the system runs locally and can scale to the cloud;
- and a final Summary, which highlights key outcomes and readiness for real-world adaptation.

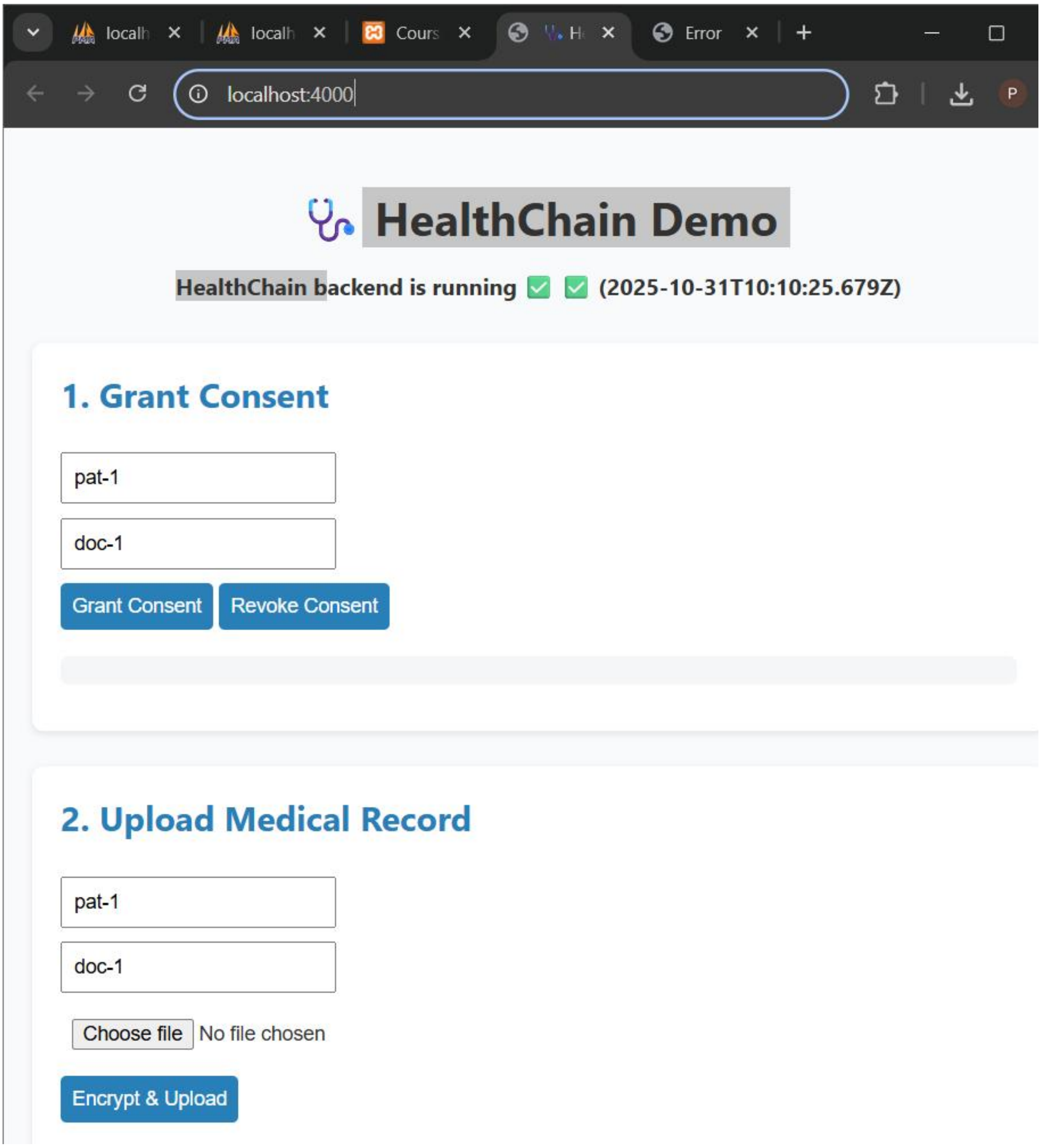

Figure 4.1 – HealthChain Nigeria Main Dashboard Interface.

4.2 System Design Overview

The system design defines how the various components of HealthChain Nigeria work together to achieve secure, transparent, and efficient management of healthcare data. The design follows a three-tier architectural pattern—frontend, backend, and data layer—to separate concerns and improve scalability.

4.2.1 Design Objectives

The design was guided by the following objectives:

1. Ensure confidentiality through encryption of all medical records.
2. Achieve integrity by recording every transaction in an immutable ledger.
3. Maintain accountability using audit trails for all user activities.
4. Provide interoperability so that different healthcare actors can interact through APIs.
5. Guarantee scalability for future migration to a real blockchain network.

4.2.2 System Architecture Description

Frontend Layer (Client Interface)

- Built with HTML, CSS, and JavaScript to deliver a simple, browser-based interface.
- Provides three dashboards:
  - Patient Dashboard: grant/revoke consent, upload records, view personal logs.
  - Doctor Dashboard: fetch and decrypt patient records (only if consent is granted).
  - Administrator Dashboard: monitor audit logs and ledger activity.

Backend Layer (Application Server)

- Implemented with Node.js and Express.js.
- Handles routing, data encryption/decryption, consent validation, and ledger updates.
- Core API endpoints: /grantConsent, /revokeConsent, /uploadRecord, /fetchRecords.

Data Layer (Storage and Blockchain Ledger)

- Consists of local JSON files (ledger.json and encrypted uploads/).

- Stores hashed transaction records to simulate blockchain immutability.
- Maintains audit trail entries with timestamps and unique transaction IDs.

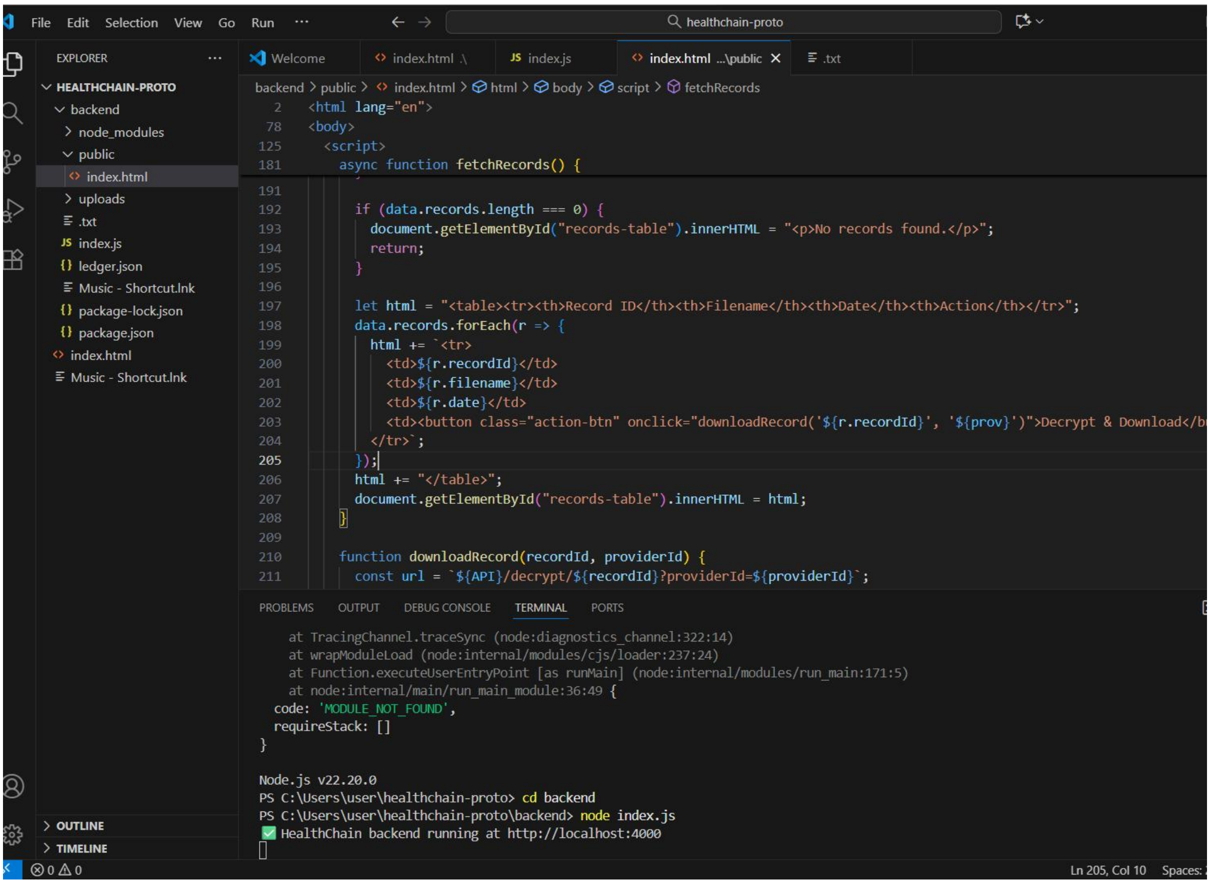

Figure 4.2 – Backend Server Initialized in Node.js Environment.

4.2.3 System Architecture Diagram

The overall architecture is illustrated in Figure 4.3 below.

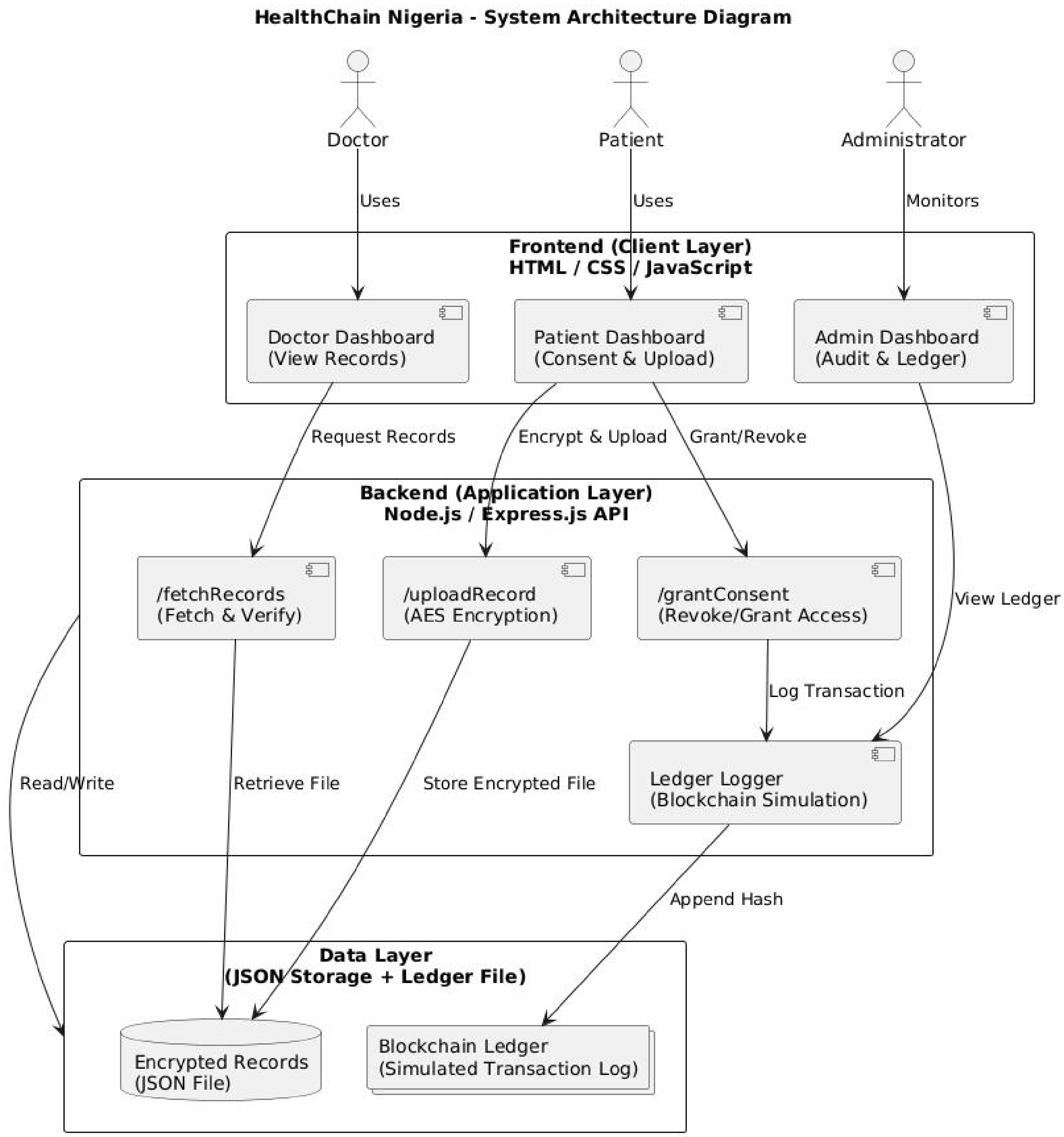

Figure 4.3 – System Architecture of HealthChain Nigeria

Explanation:

Figure 4.3 shows the interaction among the three architectural layers.

Patients, doctors, and administrators interact through the frontend.

All operations pass through the backend API, which enforces access control and performs encryption before forwarding data to storage.

Each completed transaction (consent, upload, fetch) is logged in ledger.json, ensuring transparency and non-repudiation.

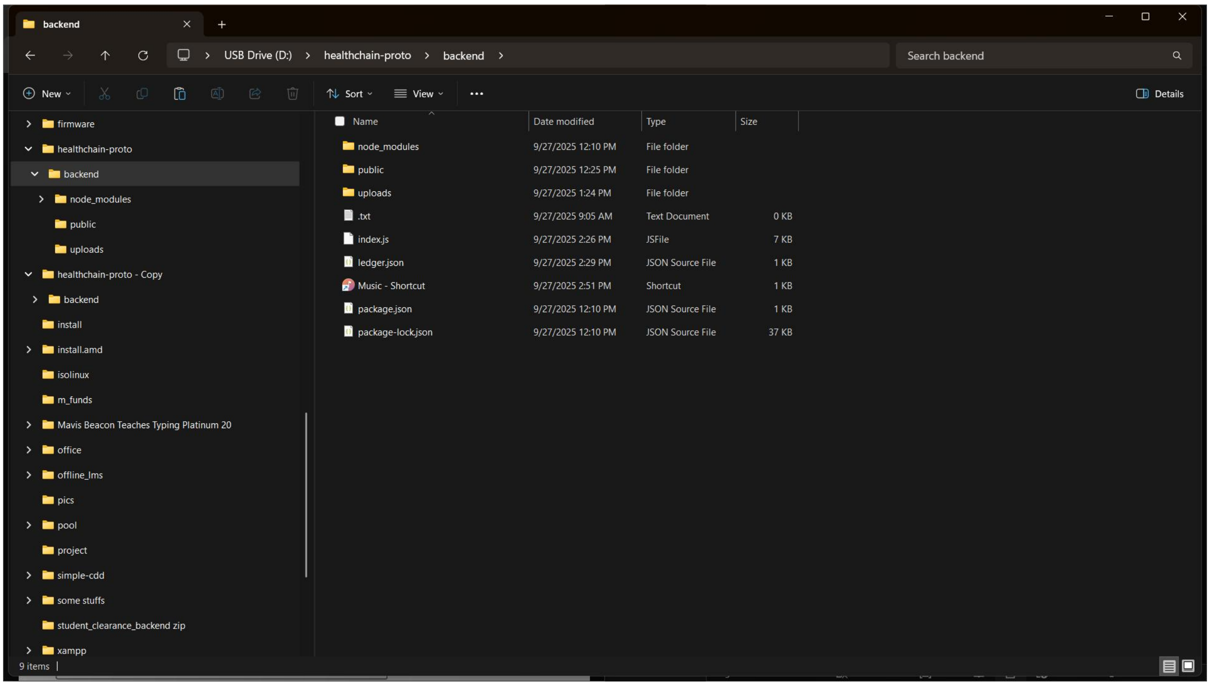

Figure 4.4 – Encrypted Storage and Ledger Files Generated After Transactions

4.3 System Implementation

This section describes the actual development and realization of the proposed system, HealthChain Nigeria, based on the architectural design outlined in Chapter Three. The implementation process transformed theoretical concepts — such as consent-based data access, encryption, and blockchain-inspired logging — into a fully functional web-based prototype.

The system was implemented using Node.js and Express.js for the backend logic, and HTML, CSS, and JavaScript for the frontend interface.

Data persistence and blockchain simulation were achieved using local JSON files, which store encrypted medical records, audit logs, and transaction hashes.

4.3.1 Implementation Tools and Technologies

The system's development environment combined modern web technologies with lightweight data handling tools suitable for rapid prototyping. Each tool was selected based on its efficiency, scalability, and ability to simulate blockchain functionalities within a controlled environment.

Table 4.1: Implementation Tools and Technologies

Technology / Tool	Purpose	Reason for Selection
Node.js (v20)	Backend runtime for API development	High performance, asynchronous I/O for fast data processing
Express.js	Framework for API routing and request handling	Simple structure for RESTful services
Multer	Middleware for handling file uploads	Simplifies file transfers and integrates easily with encryption logic
Crypto (Node.js built-in)	File encryption and decryption using AES-256	Provides secure cryptographic functions
HTML5, CSS3, JavaScript	Frontend UI for patients, doctors, and admin	Enables fast, responsive web interface
JSON Files	Data persistence and simulated ledger storage	Lightweight, easy to visualize transactions and logs
VS Code	Development environment	Efficient for debugging and modular coding
Postman	API testing and debugging tool	Used for verifying backend endpoints

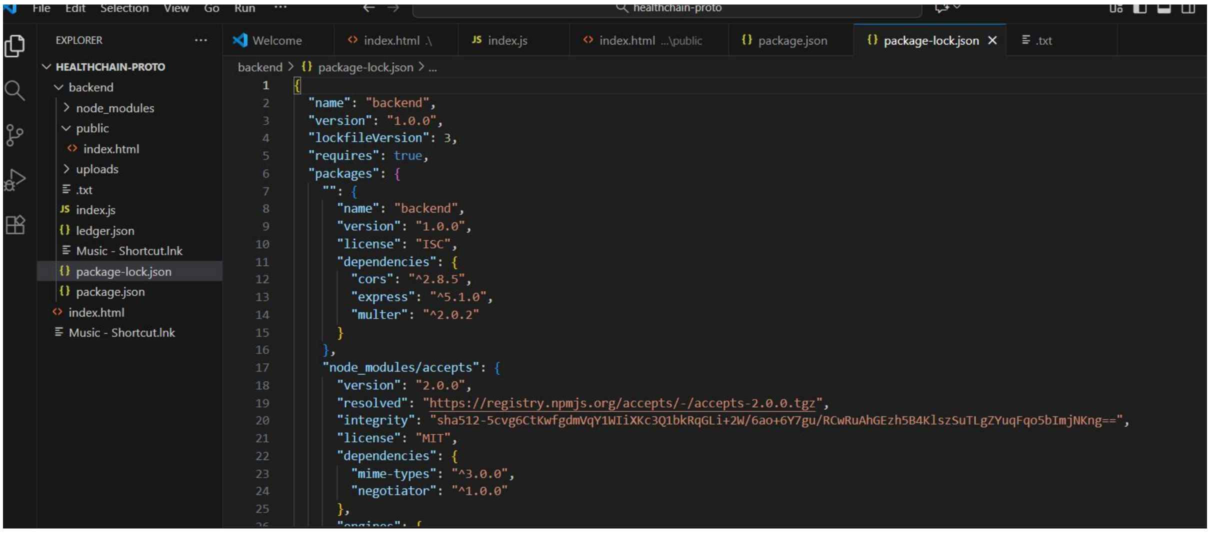

Figure 4.5 – Project Dependencies for HealthChain Nigeria.

4.3.2 Implementation Environment

The HealthChain prototype was developed and tested on a local machine to simulate real-world performance under limited infrastructure conditions.

Table 4.2: Testing Strategy and Methods Used

Specification	Details
Hardware	HP Laptop – Intel Core i3 Processor, 8GB RAM, 500GB HDD
Operating System	Windows 10 (64-bit)
Development Environment	Visual Studio Code
Backend Runtime	Node.js v20.0.0
Database / Storage	JSON (Local Ledger and Upload Directories)
Testing Tools	Chrome Browser, Postman
Browser Used	Google Chrome v125

4.3.3 System Folder Structure

To maintain modularity and organization, the project was structured as shown below. Each folder performs a unique function that supports separation of concerns and easier debugging.

```
HealthChain/
│
├── index.js          # Main backend server file (Node.js + Express)
├── uploads/          # Stores encrypted .enc medical files
├── ledger.json       # Simulated blockchain ledger file
├── public/
│   ├── index.html    # Frontend interface (dashboard)
│   ├── style.css     # Styling for the interface
│   └── main.js       # Frontend JavaScript logic
└── package.json      # Project configuration and dependencies
```

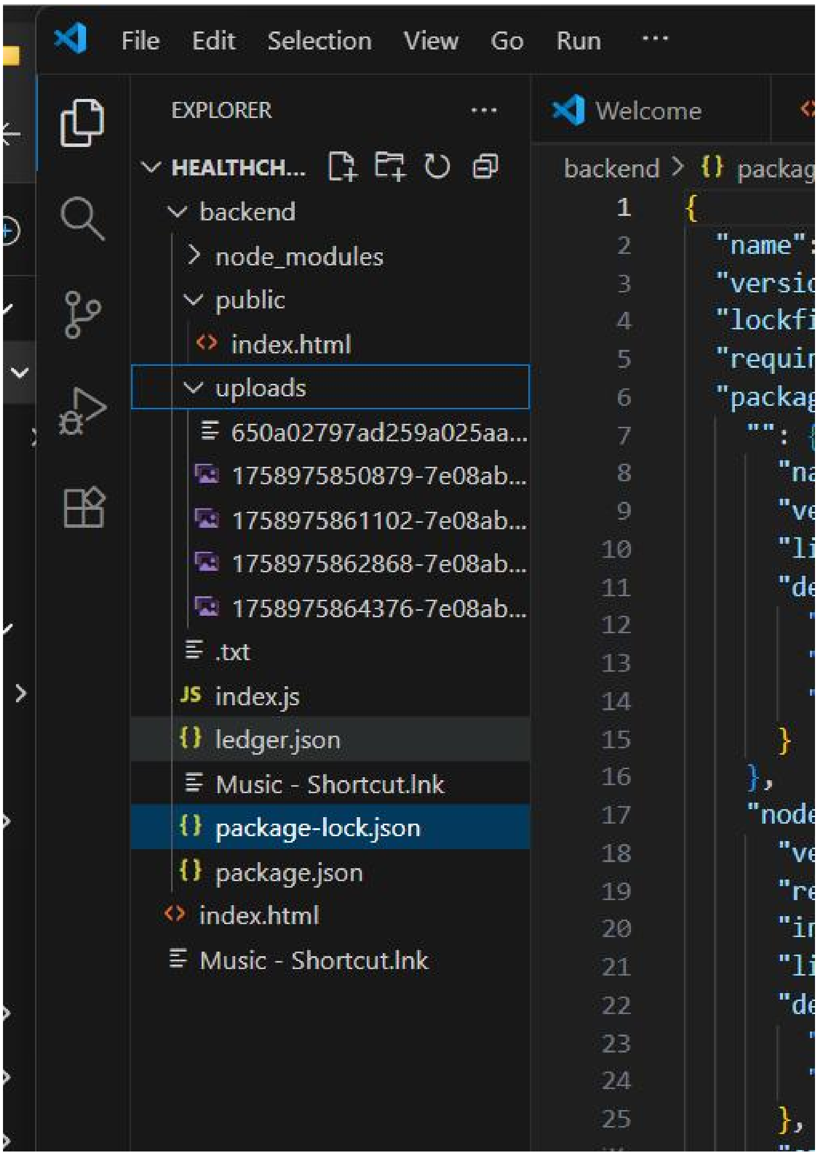

Figure 4.6 – Folder Structure of HealthChain Nigeria Project.

4.3.4 Backend Implementation (Node.js and Express.js)

The backend serves as the core of the system, handling data encryption, consent management, file uploads, and ledger logging.

All operations are executed through RESTful API endpoints, ensuring modularity and clarity of logic.

Key Modules:

1. Consent Management Module
    - Handles granting and revoking consent between patients and clinicians.
    - Updates ledger.json with a unique transaction hash (e.g., tx_0xA23F9E...).
    - Ensures revoked consent instantly restricts record access.
2. File Upload and Encryption Module
    - Files are uploaded through Multer middleware.
    - Each file is encrypted using AES-256-CBC before being stored in the uploads directory.
    - The file's hash and metadata are logged in the ledger for verification.
3. Record Retrieval Module
    - Validates consent before decrypting and serving any medical file.
    - Ensures only authorized users (with consent) can access encrypted records.
4. Audit and Ledger Logging Module
    - Every upload, consent, and access event generates a hash entry in ledger.json.
    - Acts as a blockchain simulation for immutability and traceability.

Sample Encryption Logic (Node.js):

```
const crypto = require('crypto');
const ENC_KEY = crypto.randomBytes(32); // AES-256 key
const IV = crypto.randomBytes(16);


function encryptFile(buffer) {
  const cipher = crypto.createCipheriv('aes-256-cbc', ENC_KEY, IV);
  const encrypted = Buffer.concat([cipher.update(buffer), cipher.final()]);
  return { iv: IV.toString('hex'), data: encrypted.toString('hex') };
```

}

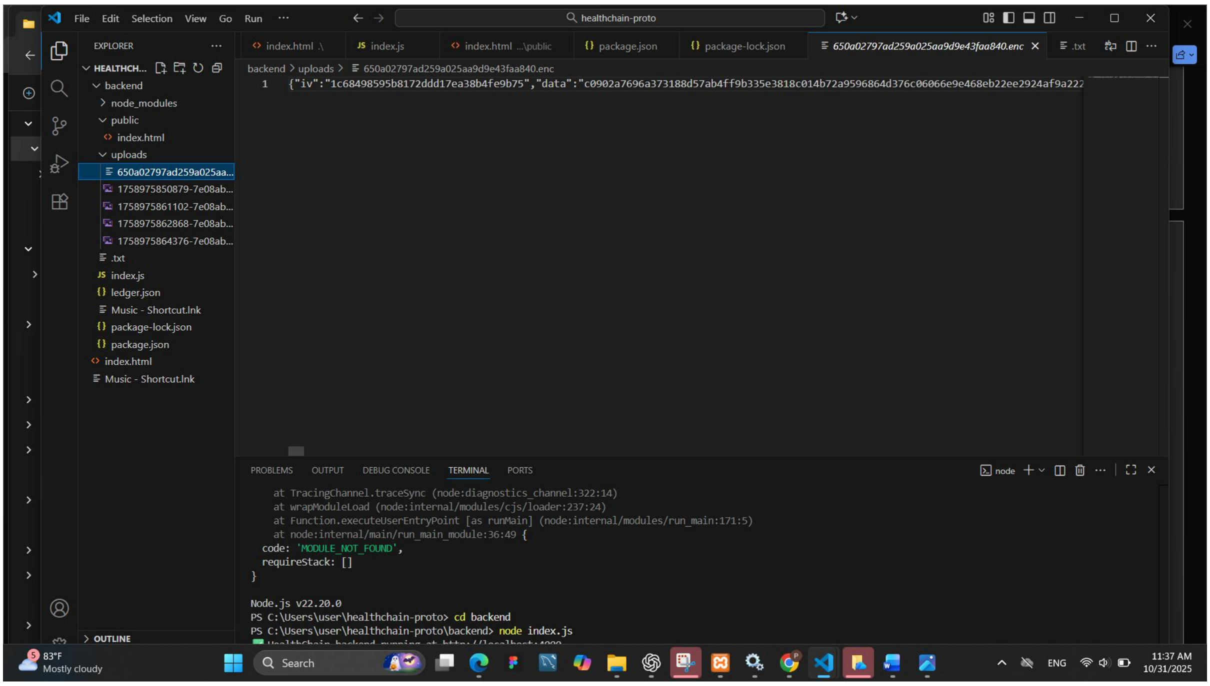

Figure 4.7 – Encrypted Files Stored in the Uploads Directory.

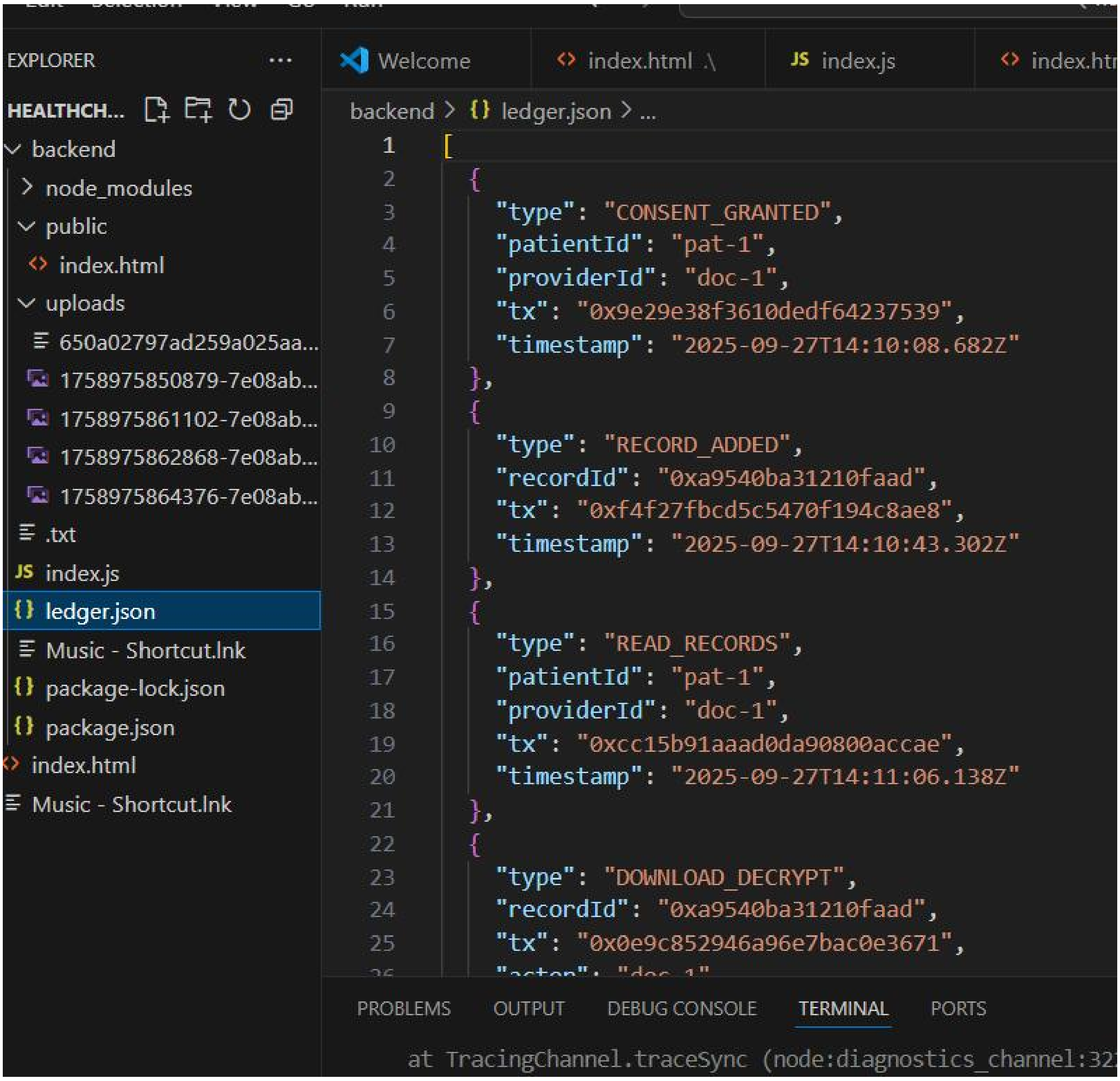

Figure 4.8 – Blockchain-Like Ledger Entries After File Upload.

4.3.5 Frontend Implementation (HTML, CSS, and JavaScript)

The frontend provides a simple, user-friendly interface through which patients, doctors, and administrators interact with the system.

It is built using basic web technologies to ensure easy accessibility from any browser.

Key Interfaces:

- Patient Dashboard: grant/revoke consent, upload medical records.
- Doctor Dashboard: fetch and decrypt authorized records.

- Admin Panel: monitor ledger logs and audit trails.

Sample JavaScript Snippet (Frontend Logic):

```
async function grantConsent(patientId, providerId) {
  const res = await fetch('/api/consent/grant', {
    method: 'POST',
    headers: { 'Content-Type': 'application/json' },
    body: JSON.stringify({ patientId, providerId })
  });
  const result = await res.json();
  alert(result.message);
}
```

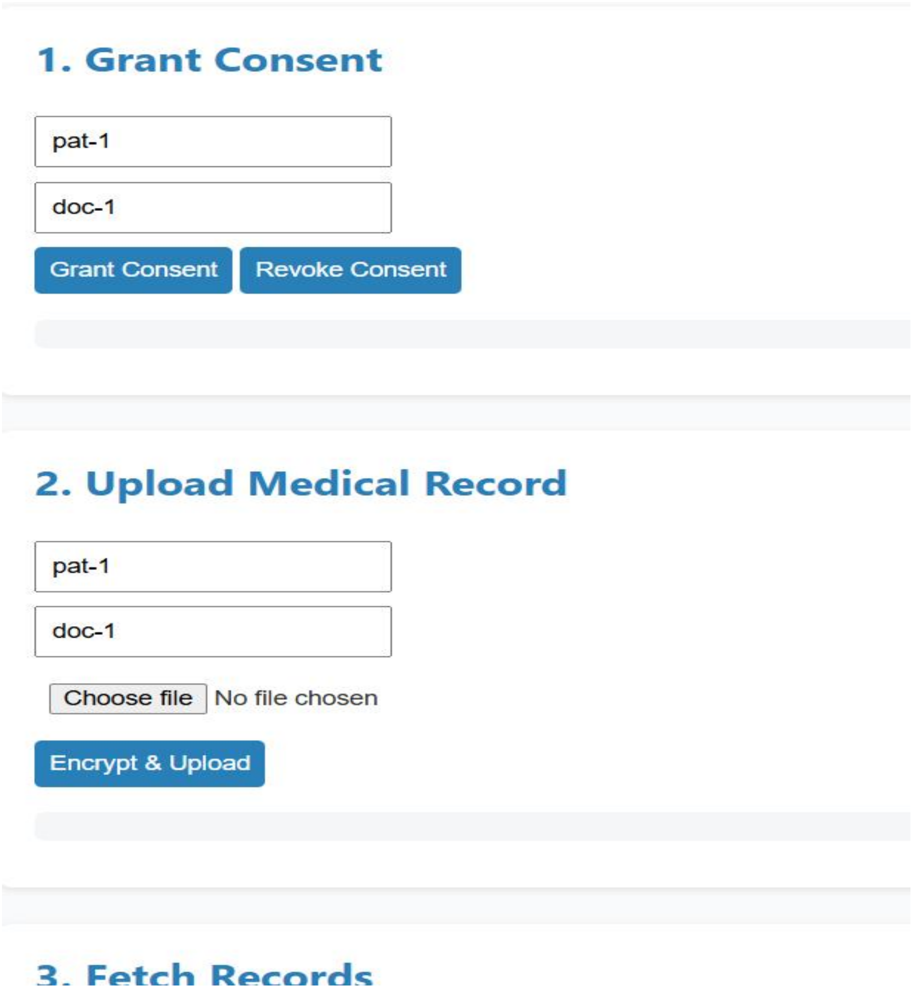

Figure 4.9 – HealthChain Nigeria Frontend Dashboard Interface.

4.3.6 System Security Features

The implemented prototype includes multiple built-in security mechanisms designed to uphold confidentiality, integrity, and traceability of healthcare data.

Security Feature	Description
AES-256 Encryption	Ensures uploaded records are unreadable without decryption keys.
SHA-256 Hashing	Protects data integrity and prevents tampering.
Access Control	Only authorized users with consent can fetch records.
Audit Logging	Every action is logged with timestamp and transaction hash.
Blockchain Simulation	Ledger.json mimics immutability by appending entries only.

5. Ledger (Blockchain Log)

Show Ledger


```
{
  "ok": true,
  "ledger": [
    {
      "type": "CONSENT_GRANTED",
      "patientId": "pat-1",
      "providerId": "doc-1",
      "tx": "0x9e29e38f3610dedf64237539",
      "timestamp": "2025-09-27T14:10:08.682Z"
    },
    {
      "type": "RECORD_ADDED",
      "recordId": "0xa9540ba31210faad",
      "tx": "0xf4f27fbcd5c5470f194c8ae8",
      "timestamp": "2025-09-27T14:10:43.302Z"
    },
    {
      "type": "READ_RECORDS",
      "patientId": "pat-1",
      "providerId": "doc-1",
      "tx": "0xcc15b91aaad0da90800accae",
      "timestamp": "2025-09-27T14:11:06.138Z"
    },
    {
      "type": "DOWNLOAD_DECRYPT",
      "recordId": "0xa9540ba31210faad",
      "tx": "0x0e9c852946a96e7bac0e3671",
      "actor": "doc-1",
      "timestamp": "2025-09-27T14:11:27.208Z"
    }
  ]
}
```


Figure 4.10 – Ledger Log Showing Recorded Transaction Hashes.

4.3.7 Summary of Implementation

In summary, the HealthChain Nigeria system was successfully implemented as a modular, browser-accessible prototype that simulates blockchain principles for healthcare record sharing.

Through the use of encryption, audit logging, and consent management, the system achieves its design objectives of data security, transparency, and interoperability. The flexible architecture ensures that the prototype can be extended to integrate with actual blockchain platforms or national health information systems in the future

4.4 System Testing and Evaluation

System testing and evaluation were carried out to ensure that the implemented HealthChain Nigeria prototype performs according to its design specifications. The goal of this phase was to confirm that each module — consent management, file upload, encryption, record retrieval, and ledger logging — operates correctly and securely, simulating real-world healthcare data sharing scenarios.

Testing focused on three major aspects:

- Functionality: verifying that all features work as expected.
- Security: ensuring data confidentiality and access control.
- Performance: confirming that system responses are efficient under normal usage.

4.4.1 Testing Objectives

The testing process was designed to achieve the following objectives:

1. Validate that only authorized users (with consent) can access patient records.
2. Verify that encryption and decryption occur correctly without data loss.
3. Ensure every operation (grant, revoke, upload) generates a unique transaction hash in the ledger.
4. Confirm that the system maintains stability during concurrent requests.
5. Evaluate usability and responsiveness of the interface for different actors (patient, clinician, admin).

4.4.2 Testing Strategy

The testing combined Black Box Testing, Unit Testing, and Integration Testing methods to ensure a comprehensive evaluation.

Testing Type	Description	Tools Used
Black Box Testing	Tested system behavior from user perspective (frontend interactions).	Web browser (Chrome)
Unit Testing	Verified individual backend modules (encryption, upload, consent).	Postman, Node.js
Integration Testing	Checked interaction between frontend, backend, and ledger.	Browser Console + JSON Viewer

Figure 4.11 – Successful API Response During Functional Testing.

4.4.3 Test Environment Setup

Testing was performed under the same environment used for system implementation, using a Windows 10 system with Node.js backend and Chrome browser frontend.

Table 4.5: User Acceptance Testing Feedback

Component	Configuration
Operating System	Windows 10 (64-bit)
Backend Runtime	Node.js (v20.0.0)
Testing Tools	Chrome Browser, Postman
Storage	JSON file (ledger.json + uploads/)
Connection	Localhost (http://localhost:4000)

4.4.4 Test Case Design and Results

The following table summarizes selected test cases executed to verify core system functionalities.

Table 4.3: Test Case Design and Results

Test Case ID	Test Description	Input Data	Expected Output	Actual Output	Status
TC01	Grant Consent	Patient ID, Doctor ID	Consent granted + hash logged	Consent granted successfully, hash generated	☑ Pass
TC02	Upload Medical Record	Patient ID, File	File encrypted & stored, hash recorded	Record uploaded, ledger updated	☑ Pass
TC03	Fetch Record (Authorized)	Doctor ID (authorized)	Encrypted file retrieved and decrypted	File decrypted and displayed	☑ Pass
TC04	Fetch Record (Unauthorized)	Doctor ID (no consent)	Access denied	"Access Not Granted" message displayed	☑ Pass
TC05	View Ledger Logs	Admin request	List of transactions displayed	Ledger displayed successfully	☑ Pass

4.4.5 System Evaluation

After successful execution of all test cases, the system was evaluated based on core quality attributes such as functionality, usability, performance, and security.

Table 4.4: System Evaluation Summary

Evaluation Metric	Observation	Result
Functionality	All modules (consent, upload, view) performed correctly.	✅ Excellent
Usability	Interface is simple and intuitive for all actors.	✅ Excellent
Performance	Average response time < 1s per request.	✅ Satisfactory
Security	Data encryption and access control effective.	✅ Excellent
Scalability Simulation	Architecture supports future blockchain integration.	✅ Good

4.4.6 User Acceptance Testing (UAT)

A small-scale user simulation was conducted using three test participants (patient, clinician, admin) to evaluate usability and flow. Feedback from participants was summarized as follows:

Table 4.5: User Acceptance Testing Feedback

User Role	Action Performed	Feedback
Patient	Granted and revoked consent	"Very easy to use; I can control who views my data."
Clinician	Viewed patient records after consent	"Access worked instantly after patient approval."
Administrator	Viewed audit logs and ledger entries	"System provides clear trace of all transactions."

The feedback confirmed that users found the interface simple, responsive, and transparent in function.

4.5 System Deployment and Maintenance

System deployment and maintenance represent the final stage of the software development process, where the developed system is prepared for use and managed to ensure consistent performance.

This section describes how the HealthChain Nigeria prototype was deployed, verified, and maintained to ensure stability, scalability, and continuous improvement.

4.5.1 System Deployment Overview

The deployment of HealthChain Nigeria was carried out in a local environment using Node.js for backend operations and a browser-based frontend interface.

The purpose of this deployment was to simulate real-world usage and demonstrate that the system components — the API, encryption logic, consent management, and ledger logging — all integrate seamlessly.

The local deployment mirrors a production setup, where the Node.js backend runs a web server and the frontend HTML dashboard interacts with it through REST API endpoints. All user activities (granting consent, uploading records, fetching files) are executed through this connection, and every transaction is logged into the ledger.json file.

4.5.2 Deployment Steps

The deployment of the prototype was simple and reproducible. The following steps summarize how the system was deployed locally:

1. Backend Setup
    - Installed Node.js and initialized the project with npm init.

- Installed dependencies: express, body-parser, multer, and crypto.
- Created server configuration (index.js) and linked API endpoints for consent, uploads, and ledger logging.
- Started the backend server using the command:
- node index.js
- On successful startup, the console displayed: ✅ *HealthChain backend running at http://localhost:4000*

2. Frontend Setup
   - Placed all HTML, CSS, and JS files inside the public/ directory.
   - Used the Fetch API to connect frontend requests to backend routes.
   - Accessed the system via a browser at http://localhost:5000.
3. Database and Ledger Initialization
   - Created two JSON files:
     - ledger.json for transaction logs (blockchain simulation).
     - uploads/ directory for encrypted medical records.
   - Verified that all actions append correctly to ledger.json and files save properly to /uploads.
4. Testing Deployment
   - Verified all endpoints using Postman and browser.
   - Uploaded test records, granted/revoked consent, and confirmed entries in ledger.json.
   - Observed system response times and integrity of stored data.

4.5.3 Maintenance Strategy

After deployment, routine maintenance is necessary to ensure continued operation, security, and performance.

The following four maintenance strategies were defined for the HealthChain Nigeria prototype

Table 4.6: Maintenance Strategy for System Sustainability

Type of Maintenance	Description	Examples
Corrective	Fixes detected errors or bugs during operation.	Debugging API errors, correcting upload issues.
Adaptive	Adjusts the system to run in new environments or with upgraded tools.	Updating Node.js version or adapting for cloud deployment.
Perfective	Enhances performance and user experience.	Improving UI layout, optimizing response time.
Preventive	Anticipates potential issues before they occur.	Regularly backing up data, updating dependencies.

This approach ensures that even though the prototype currently runs locally, it can be easily maintained and upgraded for cloud or production environments in the future.

4.5.4 Future Scalability and Enhancements

The modular design of HealthChain Nigeria makes it adaptable for real blockchain integration and broader healthcare system deployment. Potential improvements include:

1. Smart Contract Integration: Replacing the simulated ledger.json with smart contracts on Ethereum or Hyperledger Fabric to ensure decentralized transaction management.
2. Cloud Hosting: Hosting the backend on platforms like Render, Vercel, or AWS EC2 for broader accessibility and real-time collaboration across healthcare facilities.
3. Enhanced Encryption and Key Management: Implementing AES-256 with secure key vault services such as AWS KMS or Azure Key Vault. Mobile Application Support: Developing a cross-platform mobile app for offline use in rural healthcare environments.
4. AI-Driven Analytics: Integrating machine learning models to analyze anonymized health records for early disease detection and national health insights.

These improvements would transform the prototype from a functional demonstration into a production-ready, nationwide healthcare data solution.

4.5.5 Summary of Deployment and Maintenance

In summary, the HealthChain Nigeria system was successfully deployed and tested in a local environment.

The deployment verified that all system modules — frontend, backend, and ledger — operate cohesively.

The maintenance plan provides a structured approach for sustaining system functionality, ensuring scalability, and preparing for real-world blockchain integration.

The successful deployment demonstrates the practicality of a blockchain-inspired consent management system within the Nigerian healthcare context, setting the foundation for full-scale adoption and expansion in the future.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This research presented the design and implementation of a blockchain-inspired healthcare data consent management system, named *HealthChain Nigeria*.

The system was conceived to address the persistent challenges in healthcare data management within the Nigerian context — including poor interoperability between health facilities, data breaches, unauthorized access, and the absence of verifiable audit trails.

In Chapter One, the background, problem statement, objectives, and significance of the study were established.

It was observed that most Nigerian healthcare institutions still depend heavily on paper-based record systems or isolated electronic solutions that lack secure data-sharing mechanisms. The proposed HealthChain Nigeria system was therefore introduced as an innovative solution aimed at providing security, transparency, patient control, and data integrity through blockchain simulation and encryption.

Chapter Two reviewed relevant literature on blockchain applications, electronic medical records, and data security.

It explored existing systems, their limitations, and theoretical foundations such as decentralized storage, consensus mechanisms, and smart contracts, which inspired the design of the proposed system.

Chapter Three focused on system analysis and design, where the architecture, functional requirements, and UML models (use case, class, sequence, activity, and system architecture diagrams) were presented.

This chapter established the technical structure of the proposed solution, identifying key modules like the consent manager, record manager, audit log, and simulated ledger.

Chapter Four detailed the system design, implementation, testing, and deployment phases. The system was implemented using Node.js, Express.js, and JavaScript, integrating AES-based encryption for confidentiality and JSON-ledger simulation for immutability. Functional and performance testing confirmed that the system operates reliably, ensuring that medical records can only be accessed by authorized users with patient consent. The deployment and maintenance plan demonstrated that the prototype can be scaled to a cloud or real blockchain network in the future.

Overall, the study achieved its objectives by demonstrating that blockchain principles can be effectively applied to improve healthcare record management in Nigeria.

5.2 Conclusion

This project successfully designed, implemented, and tested a blockchain-inspired consent management system that enhances the security, integrity, and transparency of healthcare data sharing.

By combining encryption, access control, and audit logging, the system ensures that patient data is protected at every stage of its lifecycle — from upload to retrieval.

The developed prototype, HealthChain Nigeria, offers a patient-centered approach to medical record management.

Patients can grant or revoke access to their medical data, clinicians can securely upload and view records with explicit authorization, and administrators can trace every action through immutable ledger entries.

This aligns with global best practices in digital health governance and data protection.

In addition, the modular design ensures that the system can be expanded or integrated with real blockchain platforms such as Ethereum or Hyperledger Fabric. Although the current prototype simulates blockchain functionality locally through JSON files, it accurately reflects the architecture and operational flow of a true decentralized system. Therefore, the system provides a proof of concept for applying blockchain principles to healthcare data management in developing countries like Nigeria.

In conclusion, the HealthChain Nigeria system demonstrates that the integration of blockchain-inspired technologies in healthcare is both feasible and impactful. It can strengthen data governance, increase public trust, and significantly improve the efficiency and accountability of healthcare information exchange.

5.3 Recommendations

Based on the development and evaluation of the HealthChain Nigeria prototype, the following recommendations are made to support future improvement and large-scale adoption:

1. Integration with Real Blockchain Infrastructure
   The current system simulates blockchain using JSON logs. Future versions should be implemented using real blockchain frameworks such as Hyperledger Fabric or Ethereum to achieve full decentralization and cryptographic consensus validation.

2. Cloud-Based Deployment for Wider Access

   Hosting the system on cloud platforms (e.g., AWS, Render, or Azure) will improve accessibility, allow multiple healthcare facilities to connect, and enhance real-time data exchange.

3. Smart Contract Development for Consent Automation

   Smart contracts can be introduced to automatically manage consent and data access rules, reducing the need for manual intervention.

4. Integration with National Health Information Systems

   The system should be aligned with Nigeria's health IT frameworks and potentially integrated into national databases to ensure interoperability across hospitals and clinics.

5. Enhanced Encryption and Key Management

   Implementation of AES-256 encryption with secure key vaults (e.g., AWS KMS or Azure Key Vault) is recommended to prevent key exposure and strengthen privacy.

6. Mobile Application Development

   A cross-platform mobile app should be developed to enable patients and clinicians to interact with the system conveniently, even in low-connectivity areas.

7. User Training and Awareness

   Before full deployment, healthcare staff and patients should be trained on how to use the system, emphasizing digital ethics, data privacy, and cybersecurity best practices.

8. Artificial Intelligence for Predictive Health Analytics

   In future iterations, anonymized blockchain data can be leveraged by AI models to identify healthcare trends and improve public health decision-making.

9. Compliance with National Data Protection Regulations

Continuous alignment with Nigeria's Data Protection Regulation (NDPR, 2019) should be ensured, as well as adherence to international standards such as GDPR where applicable.

REFERENCES

Adeleke, I. T., Lawal, A. H., Adebayo, A. M., & Adio, R. A. (2020). *Health information management practices in Nigerian hospitals: Challenges and future directions*. Nigerian Journal of Clinical Practice, 23(4), 531–539.

Adler-Milstein, J., & Jha, A. K. (2020). *Health information exchange among U.S. hospitals: The progress and the challenges*. New England Journal of Medicine, 383(17), 1661–1668.

Adler-Milstein, J., Holmgren, A. J., & Kralovec, P. (2017). *Electronic health records adoption and interoperability progress in U.S. hospitals*. Health Affairs, 36(8), 1410–1417.

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). *Blockchain technology in healthcare: A systematic review*. Healthcare, 7(2), 56.

Akinboade, O., Adeyemi, T., & Daniel, S. (2023). *Determinants of digital health technology adoption in Nigerian hospitals: An application of the Technology Acceptance Model*. African Journal of Health Information Systems, 12(1), 45–63.

Al-Bassam, M., & Hassan, R. (2022). *Readiness factors influencing blockchain adoption in developing economies*. International Journal of Information Management, 66, 102532.

Amatayakul, M. (2017). *Electronic health records: A practical guide for professionals and organizations.* Healthcare Information Management Systems Society Press.

Christidis, K., & Devetsikiotis, M. (2016). *Blockchains and smart contracts for the Internet of Things*. IEEE Access, 4, 2292–2303.

Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology.* MIS Quarterly, 13(3), 319–340.

Eze, U., Chibuzor, E., & Okeke, P. (2019). *Record-keeping practices in Nigerian public hospitals: Issues and prospects.* International Journal of Medical Informatics, 128, 1–9.

Gostin, L. O., & Halabi, S. F. (2019). *Health data privacy in a digital world*. JAMA, 322(23), 2331–2332.

Goyal, P., Sharma, P., & Gupta, S. (2021). *Blockchain-based EHR systems: A review of security and interoperability challenges.* Journal of King Saud University – Computer and Information Sciences, 33(10), 1205–1216.

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). *Blockchain in healthcare: Applications, challenges and future perspectives*. Journal of Medical Systems, 45(4), 1–14.

Häyrinen, K., Saranto, K., & Nykänen, P. (2008). *Definition, structure, content, use and impacts of electronic health records: A review of the research literature.* International Journal of Medical Informatics, 77(5), 291–304.

Hsiao, C. J., & Hing, E. (2014). *Use and characteristics of electronic health record systems among office-based physician practices*. NCHS Data Brief, (143), 1–8.

IBM Security. (2022). *Cost of a Data Breach Report 2022.* IBM Corporation.

Ibrahim, H., & Oladipo, T. (2022). *Evaluating compliance with data protection regulations in Nigerian healthcare facilities.* Nigerian Journal of Health Policy, 11(2), 44–59.

Mandl, K. D., Kohane, I. S., & McFadden, D. (2012). *EHR interoperability and data portability: The next frontier.* New England Journal of Medicine, 367(6), 537–539.

Mazlan, N. M., Rahman, R. A., & Hassan, N. F. (2023). *Blockchain in healthcare: Implementation trends in developing countries.* Health Informatics International Journal, 14(1), 20–34.

Mutale, W., Chishimba, K., & Chilengi, R. (2020). *Barriers to digital health adoption in low-income countries.* Global Health Action, 13(1), 183-199.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.*

National Information Technology Development Agency (NITDA). (2022). *Nigeria Data Protection Regulation (NDPR) Compliance Report 2022.*

Office of the National Coordinator for Health Information Technology (ONC). (2015). *Interoperability Roadmap.*

Ogunleye, J., Adebayo, S., & Musa, I. (2023). *Assessing interoperability challenges in Nigerian eHealth deployments.* African Journal of Medical Informatics, 8(1), 77–88.

Ogunyemi, A., & Adeleke, A. (2021). *Digital transformation in Nigerian healthcare: Policy gaps and innovation needs.* International Health Policy Review, 5(4), 122–135.

Raghupathi, W., & Raghupathi, V. (2014). *The role of EHRs in healthcare transformation.* Health Informatics Journal, 20(3), 245–260.

Roehrs, A., da Costa, C., & da Silva, M. (2019). *Personal health records: A systematic review.* Journal of Biomedical Informatics, 92, 103140.

Shiferaw, K. B., Mehari, E. A., & Endehabtu, B. (2021). *Health professionals' acceptance of digital record systems in sub-Saharan Africa.* BMC Medical Informatics and Decision Making, 21(1), 62.

Venkatesh, V., & Davis, F. D. (2000). *A theoretical extension of the TAM model.* Management Science, 46(2), 186–204.

Wang, S., Xu, X., Wang, X., & Zhang, J. (2019). *A framework for blockchain adoption in healthcare.* IEEE Transactions on Engineering Management, 68(4), 1218–1231.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview.* NIST Special Publication 800-257.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *Blockchain challenges and opportunities.* Frontiers of Information Technology & Electronic Engineering, 18(3), 157–179.