ISSN: 3107-6513

Secured Medical Laboratory Test Results System using AES-256 Encryption Algorithm

Felix Olutokunbo Idepefo[1], Oluwabamise Joseph Adeniyi[2], Grace Chinenye Okorie[3], Christiana Jumoke Daramola[4], Bright Gazie Akwaronwu[5]

[1]Department of Computer Science, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria
[2, 3,4]Department of Software Engineering, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria
[5]Department of Information Technology, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria
[1]idepefof@babcock.edu.ng, [2]adeniyiolu@babcock.edu.ng, [3]okorieg@babcock.edu.ng, [4]daramolac@babcock.edu.ng, [5]akwaronwu0329@pg.babcock.edu.ng

Abstract:

It is estimated that 70% of medical decisions rely on laboratory results, and mistakes in interpreting these results can cause unnecessary treatments, patient anxiety, and avoidable complications. To tackle this, a Secure Medical Laboratory Test Results System was proposed in this study to allow patients to access their results easily from home/work. The system was designed using Unified Modeling Language (UML), with a responsive front end built using JavaScript and React, and a backend powered by PHP. MySQL safely stores user credentials and medical laboratory test data, which were protected with AES-256 encryption. Evaluation of the system shows that encryption took 3 to 20 milliseconds, and decryption took 3.2 to 20.7 milliseconds, showing the system handles large data quickly without slowing hospital workflows. Software Quality evaluations were excellent, with scores of 98% for functionality, 97% for performance, 96% for usability, 92% for reliability, 95% for security, and 85% for compatibility. These results demonstrate that the system is secure, dependable, and easy to use, offering an effective way to manage sensitive medical information.

Keywords: Medical Test Results, Laboratory Management System, AES-256 Encryption, Medical Test Sample

1. Introduction

Medical laboratories are fundamental to healthcare systems, providing accurate test results that form the basis of disease diagnosis, treatment, and prevention [1],[2]. Through the analysis of specimens such as blood, urine, and tissue, laboratories supply clinicians with critical information that shapes medical decisions across the continuum of patient care. In contemporary practice, laboratory testing is no longer supplementary but essential, informing not only diagnostic and therapeutic choices but also prognosis and long-term disease management [3],[4]. Physicians also depend on laboratory services for screening programs, monitoring treatment outcomes, and evaluating organ and system performance. Beyond its clinical role, laboratory testing has significant implications for healthcare economics. It is estimated that nearly 70% of medical decisions are supported by laboratory results, which directly link test reliability to the quality of care [5]. Accurate and timely results promote early detection, precise diagnosis, and effective monitoring of treatment response, thereby improving patient safety, clinical efficiency, and healthcare outcomes [6]. Conversely, misapplication or misinterpretation of test results can trigger a cascade of negative effects, such as unnecessary interventions, increased patient anxiety, excessive specialist referrals, and avoidable complications [3].

Laboratory errors, whether failures in testing, misdiagnoses, or reporting delays, represent an enduring challenge. In the United States alone, these errors were estimated to cost $200–400 million annually as early as 2001, with costs expected to have escalated alongside growing laboratory demand [7]. Addressing such errors is therefore essential for improving both clinical quality and financial sustainability. The rising volume and complexity of laboratory data underscore the importance of information and communication technologies (ICTs) in laboratory management. Among the most impactful

ISSN: 3107-6513

innovations is the Laboratory Information System (LIS), a digital platform designed to manage, process, report, and securely archive laboratory data [8]. By reducing diagnostic errors, expediting reporting, and supporting evidence-based decision-making, LIS has been shown to improve both efficiency and patient outcomes [9]. Increasingly integrated into electronic health records (EHRs), LIS provides long-term benefits for clinicians, patients, and health systems alike [6]. Despite these advantages, many laboratories in Nigeria remain dependent on paper-based systems, which are increasingly inadequate in meeting clinical demands. Manual record-keeping result in delivery delays, undermine patient outcomes, and threatens institutional credibility.

The consolidation of laboratory operations, combined with the rising demand for specimen testing, has magnified these challenges. In addition, public health surveillance and disease prevention initiatives require timely access to laboratory data needs that paper systems cannot reliably meet. Against this backdrop, the transition to digital laboratory systems is no longer optional but a necessity. Implementing LIS enhances accuracy, timeliness, and efficiency, thereby reinforcing patient safety and the overall quality of healthcare delivery. This study therefore proposes the development of a Secure Medical Laboratory Test Results System (MLTRS) that allows patients to retrieve their results securely and remotely. The system employs the AES-256 encryption algorithm to protect patient data, ensuring confidentiality and restricting access solely to authorized individuals. The Advanced Encryption Standard with a 256-bit key (AES-256) is recognized as one of the most secure symmetric encryption methods available today, offering strong resistance against brute-force attacks and unauthorized data access [10]. In the healthcare sector, AES-256 has been increasingly implemented to safeguard sensitive information, including laboratory test results, thereby ensuring confidentiality, integrity, and compliance with data protection regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and General Data Protection Regulation (GDPR) [10], [11]. Its efficiency and reliability in protecting large volumes of clinical data make it a preferred cryptographic standard for both Electronic Health Record (EHR) systems and LIS [12].

2. Review of Related Literature

Health records in general are indispensable to effective healthcare delivery, serving as the foundation for accountability, documentation of patient history, and continuity of care. Medical records contain critical data such as biographic details, diagnostic results, and treatments, making their accuracy and availability very important [13],[14],[15]. Laboratory testing is fundamental to clinical decision-making, with research suggesting that up to 70 percent of medical decisions rely on laboratory test results [5]. Traditionally, test requests have been handled manually, with physicians filling out paper-based forms that patients deliver to laboratories [16]. This manual process often results in inefficiencies such as overcrowded reception areas, slower workflows, and challenges in keeping physicians updated with the wide array of available tests. The introduction of LIS, which forms part of EHR has emerged as a vital solution, providing structured systems for managing, processing, and reporting laboratory data in a timely and reliable manner [8] [17].

Medical laboratory testing involves a multi-stage process encompassing pre-analysis, analysis, and post-analysis. These stages begin from the physician's decision to order a test, through patient preparation, sample collection, and verification, to the technical and medical validation of results before they are reported back to the physician [6]. With clinical laboratory tests underpinning much of healthcare practice [18], the adoption of information and communication technologies (ICT) has become integral to managing requests and results effectively [6]. ICT has significantly reshaped healthcare, enabling innovations such as e-Health, telemedicine, and Clinical Decision Support Systems (CDSS). These technologies enhance service delivery by improving record storage, supporting diagnostic processes, and reducing medical errors through integrated electronic alerts [19]. ERH represent a major advancement in record management, providing a comprehensive digital repository of patient data including medical history, diagnostic results, and treatment plans [20] [21]. They improve efficiency by reducing duplication of tests, minimizing transcription errors, and enabling seamless information sharing across healthcare providers.

ISSN: 3107-6513

Despite their benefits, concerns remain around patient trust, privacy, and system adoption [22]. Properly designed EHR systems can reduce inefficiencies, improve provider workflows, and strengthen patient care outcomes.

Laboratory Information Systems offer solutions by automating laboratory processes, streamlining workflows, and ensuring accurate data management. They support all phases of laboratory testing, minimize transcription errors, and improve turnaround times for results [23], [24]. LIS also facilitates collaboration between medical practitioners and laboratory staff by enabling electronic test ordering and reporting [25]. Moreover, it provides retrospective data for surveillance, such as monitoring antimicrobial resistance [26]. However, challenges such as system errors, limited functionality, and the need for competent users remain [27]. Despite these, LIS continues to play a transformative role in ensuring reliable, efficient, and accurate laboratory services that are crucial to modern healthcare delivery.

Amaechi *et al*. [28] designed and implemented an automated system aimed at addressing the challenges of handling patients' data in hospitals. Their work examined the existing information system at Our Lady of Mercy Hospital and developed an automated solution to enhance the efficiency and effectiveness of medical doctors and hospital staff in managing data. The system was reported to be accurate, flexible, secure, and efficient for its intended purpose but failed to address security. Similarly, [29] designed and implemented a Laboratory Information Management System (LIMS) for chemical analysis, adopting the Browser/Server (B/S) software architecture and a multi-layer software design based on the Zend framework. The LIMS comprised nine core modules: experimental process management, equipment management, materials management, document management, personnel management, project management, information management, system management, and login authentication. The system improved laboratory management efficiency, enhanced the reliability and authority of test reports and data, and ultimately increased the accuracy of testing outcomes. No techniques were adopted in this study to protect medical data.

Yusof and Arifin [25] proposed a new evaluation framework for Laboratory Information Systems (LIS), integrating both the laboratory testing cycle and socio-technical dimensions of LIS. Their approach combined a critical appraisal of the Total Testing Process (TTP) and the Human-Organization-Technology fit (HOT-fit) framework to identify error incidents, contributing factors, and preventive measures relevant to laboratory testing and LIS operations. Findings indicated that positive collaboration between laboratory and clinical staff facilitated smoother testing processes, reduced errors, and enhanced efficiency, while effective use of LIS further streamlined operations. The authors concluded that the TTP-LIS framework could serve as both an assessment tool and a problem-solving mechanism for laboratory testing and information systems. Furthermore, [24] highlighted the critical role of laboratory medicine during the COVID-19 pandemic and other viral outbreaks. They identified three major areas in which in vitro diagnostics provide essential contributions: etiological diagnosis, patient monitoring, and epidemiologic surveillance. The study concluded that significant investments in conventional laboratory resources, the strengthening of regional laboratory networks, the deployment of mobile laboratories, and the establishment of emergency laboratory facilities are crucial to ensuring early diagnosis, effective patient management, and therapeutic monitoring in response to global health emergencies such as COVID-19.

The Advanced Encryption Standard using a 256-bit key (AES-256) has become an essential tool in securing sensitive patient data, owing to its proven strength against brute-force attacks and its wide adoption in strong cryptographic libraries [30]. Recent research in healthcare highlights the use of AES-256 to safeguard health information (PHI) within database systems and medical record repositories. This approach not only helps minimize data exposure risks but also ensures compliance with regulations such as HIPAA, while maintaining efficient operational performance [31], [32]. A 2024 study across several healthcare facilities reported the use of AES-256 for protecting personal health information and personally identifiable information (PII), achieving a near-complete reduction in data exposure incidents while maintaining acceptable processing speeds [33]. In a similar 2023 hospital case study, the use of

ISSN: 3107-6513

AES-256 to encrypt data at rest, along with secure transmission via TLS, effectively prevented breaches of sensitive patient records while ensuring full compliance with HIPAA audits [34].

Although existing studies emphasize the importance of LIS and AES-256 encryption in protecting patient data and enhancing laboratory operations, there is limited research on systems that allow secure patient access to laboratory test results. Few studies explore how AES-256 can be practically integrated with LIS to enable remote, real-time retrieval of results while simultaneously ensuring operational efficiency, minimizing errors, and maintaining regulatory compliance. This gap is especially pronounced in developing countries like Nigeria, highlighting the need for solutions that balance data security, patient accessibility, and laboratory performance. To address this need, this study proposes a Secure Medical Laboratory Test Results (MLTRS) that allows patients to securely access their laboratory results remotely. By leveraging AES-256 encryption to protect sensitive data and integrating seamlessly with existing LIS, the system aims to improve accuracy, efficiency, and adherence to healthcare regulations.

3. Proposed Methodology

The review encompassed a diverse range of materials, including scholarly journals, academic books, and prior research studies, supplemented by insights from reputable online sources. The existing medical laboratory test result operations at Barnes Hospital, Lagos, Nigeria were studied in detail, and both the strengths and shortcomings of the current system were identified. Data were gathered through direct observation and interviews with hospital staff, ensuring that the findings reflect the realities of day-to-day practice. Building on these findings, a new system, called the Secure Medical Laboratory Test Results Management System, was proposed. The system is intended to strengthen healthcare delivery by supporting key tasks such as disease detection, accurate diagnosis, and monitoring of treatment progress. It will handle the core functions of laboratory information management, including maintaining patient records, managing laboratory tests, and processing results. The design also incorporates automation, making it possible to securely store patient data, record test samples electronically at the point of collection, and enter them directly into the database. The system will make it easier for patients, healthcare providers, and other authorized personnel to access test results quickly and reliably. The design was modelled with Unified Modeling Language (UML), while the implementation was carried out using PHP and MySQL. To protect sensitive information, both passwords and medical test results were encrypted using the AES-256 encryption algorithm, ensuring that only the rightful owner can decrypt and download medical test results. The system underwent rigorous stress testing under varying load conditions to assess its performance, stability, and scalability. User evaluation was conducted using an online questionnaire designed to evaluate key system attributes, including functionality, performance, compatibility, usability, reliability, and security to obtain a comprehensive understanding of the system's effectiveness and user satisfaction. A pilot study of the survey was performed before the full-scale survey to validate the reliability of the questionnaire, with Cronbach's Alpha (α) employed as the reliability metric. Additionally, the AES-256 encryption algorithm was evaluated in terms of encryption and decryption time to ensure secure and efficient handling of sensitive data.

4. Proposed Secure Medical Laboratory Test Results Management System Overview

This study focuses on the development of a web-based Secure Medical Laboratory Test Results System to support essential healthcare activities such as disease detection and diagnosis. The system was designed to manage core laboratory operations by automating routine tasks such as patient registration, test sample collection, result recording, and retrieval. It achieves this by electronically storing patient data, recording test samples at the point of collection, and entering results directly into a secure database. It allows clinicians and laboratory personnel to track patient records, view past medical test results, and access laboratory results reliably. Secure access controls were provided for medical laboratory scientists, nurses, and other staff, while sensitive data such as passwords and medical test results were protected using AES-256 encryption. Different user roles were incorporated to support specific functionalities. Administrators can create, edit, or delete staff and patient accounts, create new medical tests, and search for patients. Nurses can register patients, update patient records, and search

ISSN: 3107-6513

for patients. Laboratory Scientists can record sample collection data, upload and encrypt medical test results, prepare and manage medical test bills and invoices. Patients can decrypt, view, download and print their medical test results, test histories, and bill receipts. The accounts/payment unit can accept payments and generate bill receipts.

The implementation of the system involved the integration of multiple technologies to ensure efficiency, scalability, and security. The front end was developed using modern technologies, including JavaScript (both Vanilla and React) to provide a responsive and interactive user interface. PHP was used for backend development due to its ability to handle dynamic content efficiently, compatibility with various web servers, and strong community support that facilitates rapid development and customization. MySQL, a robust relational database management system, was employed to store user authentication (sign-up and login credentials) and medical test results. The web-based application will run on the XAMP platform.

5. Requirement Analysis

The requirements analysis phase establishes the foundation for developing a robust and user-focused web-based Secure Medical Laboratory Test Results System. The functional requirements define the essential capabilities expected from different users, including administrators, nurses, laboratory scientists, and patients. In contrast, the non-functional requirements specify critical aspects related to the system's performance, availability, reliability, data integrity, and security, ensuring that medical test results are managed efficiently and accessed safely.

5.1 Functional Requirements

Functional requirements define the specific capabilities and behaviors that the system must provide for different users.

Table 1: Functional Requirements of the Secure Medical Laboratory Test Results Management System

MLTRS-FRID	FUNCTIONAL REQUIREMENT DESCRIPTION
MLTRS-FR1	The system must allow administrators to create, edit, and delete staff and patient accounts.
MLTRS-FR2	The system must allow administrator and other users to securely log in and reset their passwords
MLTRS-FR3	The system must allow administrators to define, manage, and update medical test types and parameters.
MLTRS-FR4	The system must enable administrators to search for and retrieve patient records.
MLTRS-FR5	The system should provide reporting functionalities to monitor system usage and administrative activities.
MLTRS-FR6	The system must allow nurses to register new patients and update patient records.
MLTRS-FR7	The system must enable nurses to schedule sample collection and manage patient appointments.
MLTRS-FR8	The system must allow nurses to search for and retrieve patient data accurately.
MLTRS-FR9	The system must allow laboratory scientists to record sample collection details at the point of collection.
MLTRS-FR10	The system must enable laboratory scientists to upload, encrypt, and manage medical test results.
MLTRS-FR11	The system must allow laboratory scientists to generate and manage bills and invoices for tests conducted.
MLTRS-FR12	The system must allow patients to securely decrypt, view, download, and print their medical test results and histories.
MLTRS-FR13	The system must allow patients to access billing information and receipts.
MLTRS-FR14	The system must notify patients when test results are available.
MLTRS-FR15	The system must allow accounts personnel to accept payments and generate receipts.
MLTRS-FR16	The system must maintain a history of payments linked to patients' test records.

5.2 Non-Functional Requirement

Non-functional requirements define the quality attributes, performance standards, and operational constraints that ensure the Medical Laboratory Test Results Information System operates efficiently, securely, and reliably.

Table 2: Non-Functional Requirements for the Secure Medical Laboratory Test Results Management System

TYPES OF NFRs	MLTRS-NFR-ID	NON-FUNCTIONAL REQUIREMENT DESCRIPTIONS
Security	MLTRS-NFR1	The system must authenticate users using a login ID and password before granting access.
	MLTRS-NFR2	The system must ensure sensitive data, including medical test results and

ISSN: **3107-6513**

		passwords are encrypted using the AES-256 encryption algorithm.
	MLTRS-NFR3	The system must ensure verification mechanisms are in place to detect any unauthorized modifications to medical test results.
	MLTRS-NFR4	The system must ensure adherence to data protection regulations, local data laws, and international privacy standards.
Performance	MLTRS-NFR7	The system should handle at least 1,000 concurrent users without significant performance degradation.
	MLTRS-NFR8	The system must ensure that content retrieval and search results are returned within 2–3 seconds.
	MLTRS-NFR9	The system must ensure that encryption and verification do not increase file upload or download times by more than 10% compared to baseline performance.
	MLTRS-NFR10	The system should provide fast and responsive interactions, including quick uploads and downloads of test results.
Scalability	MLTRS-NFR11	The system architecture must allow horizontal scaling to accommodate an increasing number of users and storage requirements.
	MLTRS-NFR12	The system should ensure that storage, compute, and network resources are dynamically scaled to meet system demand.
Reliability	MLTRS-NFR13	The system must ensure 99.9% uptime for uninterrupted access to medical laboratory test results.
	MLTRS-NFR14	The system must recover from failures within 5 minutes using backup and restore processes.
	MLTRS-NFR15	The system must ensure file integrity is maintained during recovery, with AES-256 encryption re-verified after restoration.
	MLTRS-NFR16	The system must ensure that no data loss occurs during failures beyond the last automated backup window.
	MLTRS-NFR17	The system should ensure that fault tolerance mechanisms ensure automatic failover in the event of server or storage failures.
Usability	MLTRS-NFR21	The system must have an intuitive, responsive, and user-friendly interface that requires minimal training for administrators, nurses, laboratory scientists, accounts personnel, and patients.
	MLTRS-NFR22	The system must be accessible on multiple devices, including desktops, tablets, and smartphones.
	MLTRS-NFR23	The system should notify patients when their medical test results have been uploaded and are ready.
Compliance	MLTRS-NFR25	The system must ensure adherence to data protection regulations, local data and international privacy laws.
	MLTRS-NFR26	The system must comply with accessibility standards, including Web Content Accessibility Guidelines (WCAG) and other relevant professional regulations.

6. System Design

The Use case diagram was used to model the system. The Actors in the Secure Medical

ISSN: 3107-6513

Laboratory Test Results Management System, their roles, Preconditions, main flow, and postconditions are:

(a) Actors and their Use Cases

- **Administrator**: Manage staff and patient accounts (create, edit, delete), manage medical tests, search patient records, generate reports, log in, and reset passwords.
- **Nurse**: Register, login, reset password, Register and update patient records, Schedule sample collection, Search patient records.
- **Laboratory Scientist**: Register, log in, reset password, record sample collection, upload and encrypt test results, generate and manage bills.
- **Patient**: Register, login, reset password, view, download, and print test results, access billing information, receive notifications for test results.
- **Accounts/Payment Unit**: Register, Login, accept payments, generate receipts.
- **System**: Authenticate users, encrypt sensitive data using the AES encryption algorithm, provide notifications, Backup and restore data.

(b) Preconditions

- All users must be registered and authenticated in the system.
- Users must have appropriate role-based permissions to access their respective functionalities.
- The system and database must be accessible and operational.

(c) Main Flow (Normal Scenario)

1. The administrator logs in using credentials encrypted and verified via the AES algorithm.
2. The administrator creates a new patient account and assigns a nurse and a laboratory scientist to the patient.
3. The nurse logs in and registers patient details, schedules sample collection, and records patient history.
4. At the scheduled time, the laboratory scientist records the sample collection, uploads and encrypts medical test results, and other sensitive data using AES before storage.
5. The system stores the AES-encrypted test results and associated metadata (patient ID, test type, date) securely in the database.
6. The accounts/payment unit logs in to process payments and generate receipts for the patient.
7. The patient logs in, receives a notification of completed test results, and accesses, downloads, or prints their results securely.
8. The system decrypts the AES-encrypted test results and verifies integrity before displaying them to the patient.
9. Administrators can search patient records, manage staff accounts, and generate system reports at any time.
10. The system continuously backs up data and sends notifications for completed tests, billing updates, or system alerts.

(d) Postconditions

- All patient records, sample collections, and test results are securely stored and AES-encrypted.
- Patients can access authentic and untampered test results and billing information.
- All payments and receipts are securely logged and traceable.
- Any system or data integrity issues are logged and flagged for administrative review.

The use case diagram is shown in Figure 1.

7. Implementation of the Proposed System

The Secure Medical Laboratory Test Results Management System is designed to improve healthcare operations by efficiently managing patient data, medical tests, and reports. It comprises five main modules: registration, login, admin, patient, staff, and report summary. The registration module captures patient information securely, while the login module ensures authenticated access. The admin module allows management of staff and

ISSN: 3107-6513

patient accounts, medical tests, and records. The patient module enables viewing, decrypting, and printing test results, while the staff module is designed for nurses, laboratory scientists, and billing personnel to perform their respective duties, including processing, uploading, and encrypting tests, managing patient care, and handling payments. The report summary module allows all users to generate, view, and print test results, histories, invoices, and receipts. Data entry is primarily via keyboard, and outputs include medical results and billing documents, displayed on-screen or printed.

The system uses JavaScript (Vanilla and React) for a responsive front end, PHP for backend processing, and MySQL for secure data storage. Security measures include AES-256 encryption and role-based access control. The system underwent rigorous unit, integration, and system testing, as well as user evaluations to ensure functionality, performance, compatibility, usability, reliability, and security. Overall, the system enhances healthcare delivery by providing secure, accurate, and timely access to medical test results, streamlining laboratory operations, improving record-keeping, and supporting efficient management of patient data and hospital workflows.

Some of the snapshots of the implementation are shown in Figure 2, 3, 4, 5 and 6.

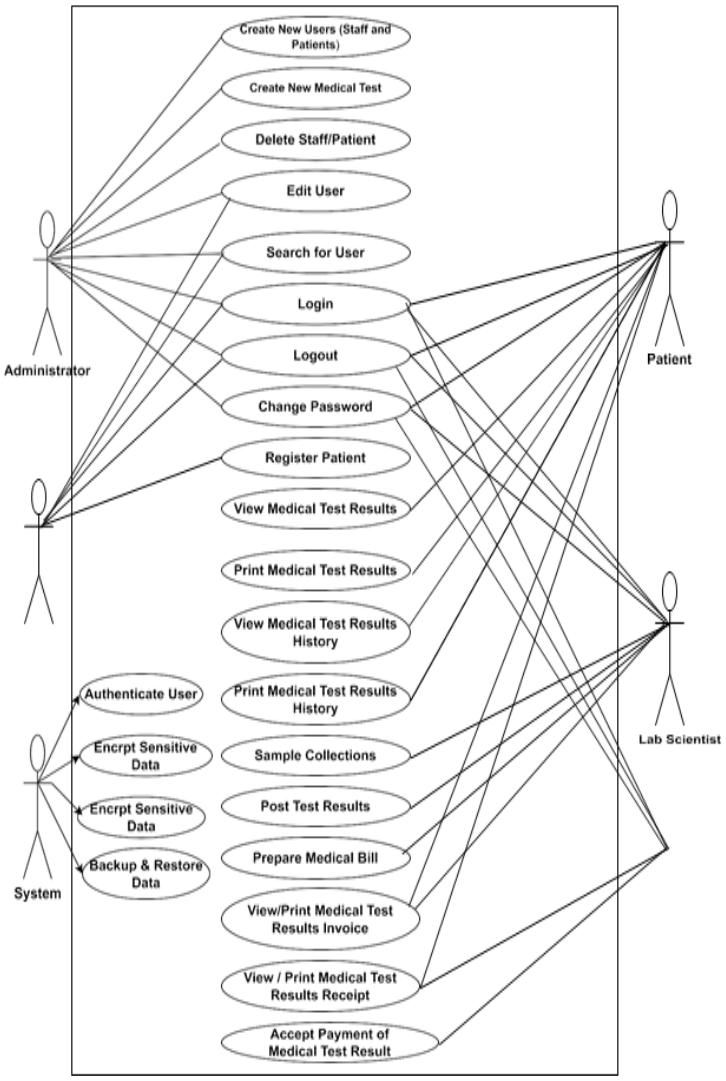

Figure 1: Use Case diagram for the Secure Medical Laboratory Test Results Management System

Figure 2.0: Home Page

ISSN: 3107-6513

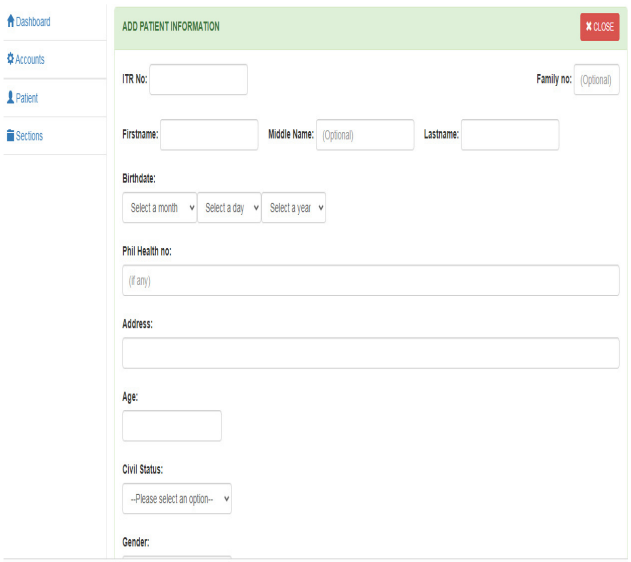

Figure 3: Patient Registration

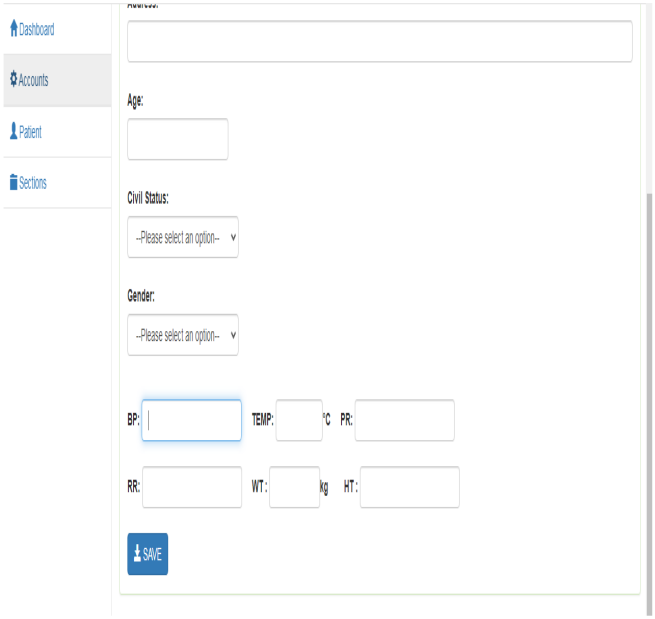

Figure 4: Test Sample Collection

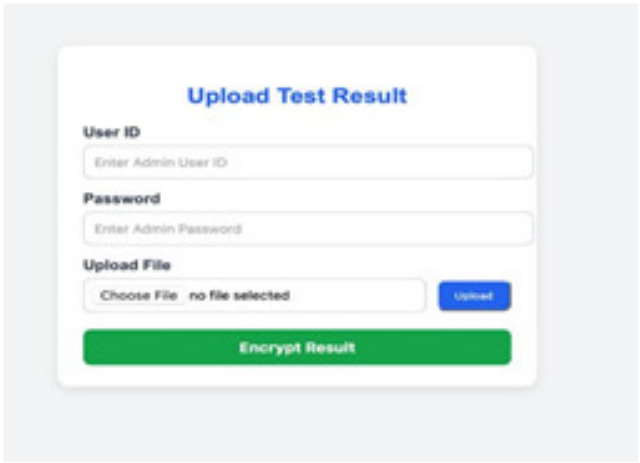

Figure 5: Upload Medical Test Results Page used by Medical Laboratory Scientist

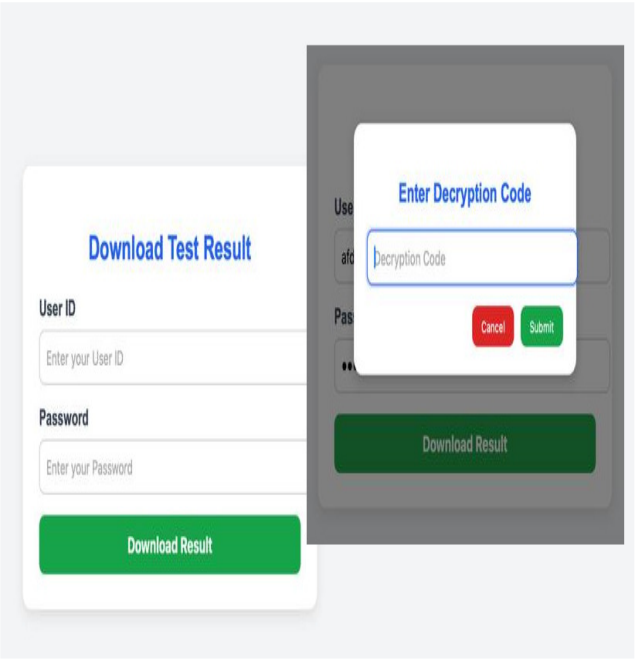

Figure 6: Download Medical Test Results Page used by the Patient

8. Results and Discussion of Results

This study presents a Secure Medical Laboratory Test Results Management System designed to enhance patient care and streamline healthcare operations through digital integration. The platform rigorously verifies and validates all user input to ensure data accuracy with immediate notifications provided in case of errors. Patient information is captured and stored to create individual patient accounts, with each patient assigned a unique Patient Identity (ID) for seamless tracking of medical and test result records. The system automatically generates detailed test report summaries and billing invoices in a clear and accessible format. Authorized users, including nurses, laboratory scientists, and patients, can monitor medical test results and billing histories in real time, promoting transparency and facilitating effective communication among healthcare providers.

User feedback reflects predominantly positive experiences, highlighting the system's intuitive interface, ease of use, and convenience. Beyond operational efficiency, the platform advances digital healthcare innovation by integrating patient management, test monitoring, and billing into a single solution, supporting data-driven decision-making and improved coordination. The system demonstrates significant potential to enhance the

ISSN: 3107-6513

quality of care, reduce administrative burden, and serve as a model for the adoption of digital technologies in modern healthcare delivery.
Evaluation details of the proposed system are provided in sections 8.1, and 8.2

8.1.Evaluation of the AES–256 Encryption Algorithm

Medical laboratory test results obtained from Barnes Hospital, Lagos, Nigeria were anonymized to prevent them from being traced back to an individual or specific source by replacing the patient's name with fictitious names. The goal is to protect personal or sensitive information by removing or altering identifiers that could reveal a person's identity. The medical test results were encrypted using AES-256 on a Core i5 computer with a processor speed of 4.33Ghz. The encryption and decryption times were obtained. Ten (10) of the results are shown in Table 3 and Figure 6.

The results indicate a clear linear relationship between file size and encryption/decryption time, with larger files requiring proportionally more time. While encryption and decryption times are very close, minor differences (0.2–0.7ms) are observed due to small system variations, which is normal for symmetric encryption algorithms like AES-256. On a Core i5 processor at 4.33GHz, encryption and decryption were efficient, ranging from 3.0–20.0ms for encryption and 3.2–20.7ms for decryption. These findings confirm that AES-256 provides robust security while maintaining fast processing, making it suitable for a Secure Medical Laboratory Test Results Management System. The linear increase in time with file size also suggests that the algorithm can manage larger datasets without significant delays.

Table 3: Encryption and Decryption Time of AES-256 Encryption Algorithm

Patient ID	Patient Name	Test Type (Sickness)	File Size (MB)	Time to Encrypt (ms)	Time to Decrypt (ms)
BAN-2025-001	John Doe	Malaria Parasite Test	0.3	3.0	3.2
BAN-2025-002	Mary Johnson	Tuberculosis Sputum Test	0.5	5.0	5.3
BAN-2025-003	Ahmed Bello	HIV ELISA Test	1.0	10.0	10.5
BAN-2025-004	Sarah Okeke	Hepatitis B Surface Antigen Test	0.8	8.0	8.4
BAN-2025-005	David Smith	COVID-19 PCR Test	2.0	20.0	20.7
BAN-2025-006	Fatima Yusuf	Typhoid Widal Test	0.6	6.0	6.3
BAN-2025-007	Michael Adams	Diabetes (Fasting Glucose Test)	0.4	4.0	4.2
BAN-2025-008	Grace Brown	Anemia Blood Test	1.1	11.0	11.6
BAN-2025-009	James Wilson	Pneumonia Chest X-ray Report	1.7	17.0	17.6
BAN-2025-010	Chika Nwosu	Cholesterol Lipid Profile	0.7	7.0	7.4

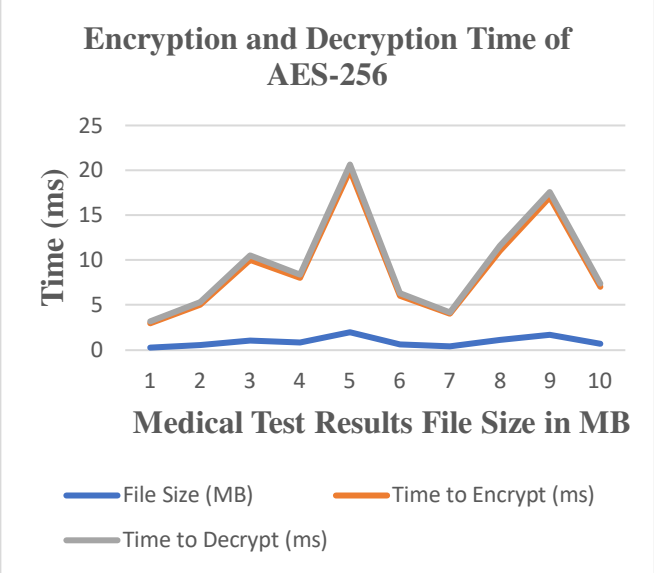

Figure 6: Encryption and Decryption Time of AES-256 Encryption Algorithm

8.2.Evaluation of Software Quality Attributes

The Secure Medical Laboratory Test Results Management System was also evaluated for

ISSN: 3107-6513

functionality, performance, compatibility, usability, reliability, and security using an online questionnaire that uses a 5-point Likert scale. The internal consistency of the questionnaire was examined using Cronbach's alpha, which quantifies the internal consistency on a standardized scale from 0 to 1. The analysis yielded a coefficient of $\alpha = 0.906$, which exceeds the commonly accepted threshold of 0.70, thereby demonstrating a high level of reliability that indicates that the questionnaire is highly dependable and that the collected data can be confidently trusted. This result confirms that the measurement metrics are consistent and that the instrument can be considered a valid and trustworthy tool for data collection. The detailed evaluation results for functionality, performance, compatibility, usability, reliability, and security are presented in Table 4 and illustrated in Figure 7.

The evaluation results across several key attributes, with results expressed as percentages, show that functionality scored 98%, reflecting the system's comprehensive support for encryption, decryption, file management, and access control, with only minor limitations. Performance received 97%, as AES-256 encryption and decryption remained fast even for larger files, with negligible delays. Compatibility was rated 85%, indicating that the system works well on standard desktop computers and integrates effectively with common laboratory software, though minor issues may occur with legacy systems. Usability scored 96%, highlighting a user-friendly interface that allows staff and patients to manage and secure files easily with minimal training. Reliability achieved 92%, demonstrating mostly consistent and predictable system behavior with very rare or negligible failures. Security, a critical aspect of managing sensitive medical data, was rated 95%, reflecting the strong protection provided by AES-256 encryption. Overall, the system is efficient, secure, and user-friendly, suitable for managing sensitive medical test results.

Table 5.0: Software Quality Attributes Evaluation

Software Quality Attributes	Value (%)
Functionality	98
Performance	97
Compatibility	85
Usability	96
Reliability	92
Security	95

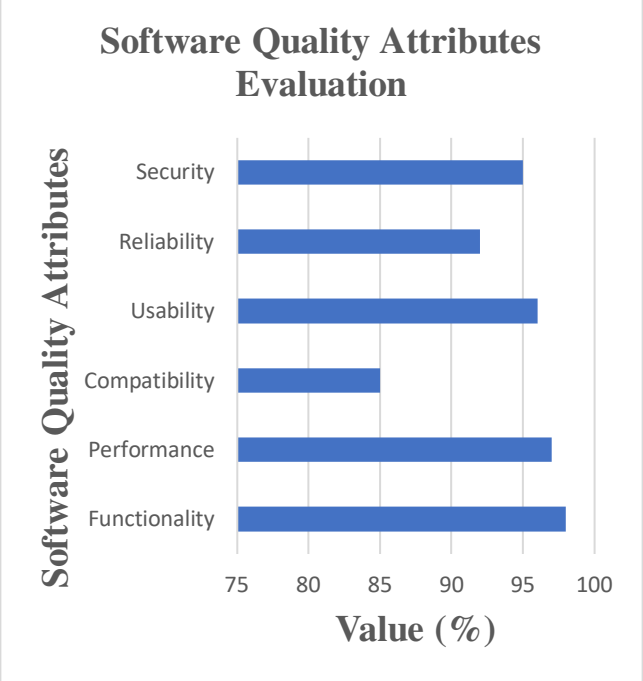

Figure 7: Software Quality Attributes Evaluation

9. Conclusion

Hospitals today are constantly balancing the need to reduce costs to provide high-quality care. One way to help achieve this balance is through a Secure Medical Laboratory Test Results Management System. Such a system can prevent unnecessary tests, reduce the risk of medical errors, give patients faster access to their results, and improve communication between medical laboratory scientists, nurses, and patients. Anonymized test results were encrypted using AES-256 on a standard Core i5 processor. Encryption times ranged from just 3 to 20 milliseconds, with decryption taking 3.2 to 20.7 milliseconds, showing that the system can handle large amounts of data quickly and securely without slowing hospital operations. The software quality attributes evaluation shows that the system performed exceptionally well. It scored 98% for functionality, 97% for performance, 96% for usability, 92% for reliability, 95% for security, and 85% for compatibility. These results suggest that the developed system is a secure, reliable, and user-friendly tool for managing sensitive medical information. To make the system better in the future, data security can be strengthened through updated encryption, multi-factor authentication, and detailed audit trails. Interoperability with other hospital systems and electronic health records can streamline workflows and reduce duplicated effort.

Finally, adding analytics and reporting features would help track test trends, turnaround times, and patient outcomes, giving hospital administrators the insight they need to make smarter, data-driven decisions.

References

[1] D. J. Hamel, J. L. Sankalé, J. O. Samuels, A. D. Sarr, B. Chaplin, E. Ofuche, and P. J. Kanki, "Building laboratory capacity to support HIV care in Nigeria: Harvard/APIN PEPFAR, 2004–2012," *African Journal of Laboratory Medicine*, vol. 4, no. 1, pp. 1–10, 2015. [Online]. Available: https://journals.co.za/doi/abs/10.4102/ajlm.v4i1.190

[2] I. V. Jani, B. Meggi, O. Loquiha, O. Tobaiwa, C. Mudenyanga, A. Zitha, and L. Vojnov, "Effect of point-of-care early infant diagnosis on antiretroviral therapy initiation and retention of patients," *AIDS*, vol. 32, no. 11, pp. 1453–1463, 2018. [Online]. Available: https://journals.lww.com/aidsonline/FullText/2018/07170/Effect_of_point_of_care_early_infant_diagnosis_on.8.aspx

[3] M. D. Krasowski, D. Chudzik, A. Dolezal, B. Steussy, M. P. Gailey, B. Koch, and J. A. Klesney-Tait, "Promoting improved utilization of laboratory testing through changes in an electronic medical record: experience at an academic medical center," *BMC Medical Informatics and Decision Making*, vol. 15, no. 1, p. 11, 2015. [Online]. Available: https://link.springer.com/article/10.1186/s12911-015-0137-7

[4] MedlinePlus, "How to Understand Your Lab Results," 2025. [Online]. Available: https://medlineplus.gov/lab-tests/how-to-understand-your-lab-results/

[5] T. M. Mtonga, F. E. Choonara, J. U. Espino, C. Kachaje, K. Kapundi, T. E. Mengezi, and G. P. Douglas, "Design and implementation of a clinical laboratory information system in a low-resource setting," *African Journal of Laboratory Medicine*, vol. 8, no. 1, pp. 1–7, 2019. [Online]. Available: https://journals.co.za/doi/abs/10.4102/ajlm.v8i1.841

[6] F. G. Luna, I. H. Contreras, A. C. Guerrero, and F. B. Guitarte, "Integrating electronic systems for requesting clinical laboratory test into digital clinical records: design and implementation," *Health*, vol. 9, no. 4, pp. 622–639, 2017. [Online]. Available: https://www.scirp.org/journal/paperinformation?paperid=75460

[7] A. F. Igila, "Quality assurance in medical laboratories in developing countries: assessment of pre-analytical errors in a chemical pathology laboratory in a tertiary hospital in Nigeria," *Journal of Health and Medical Sciences*, vol. 3, no. 1, 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3513816

[8] B. Aldosari, H. A. Gadi, A. Alanazi, and M. Househ, "Surveying the influence of laboratory information system: an end-user perspective," *Informatics in Medicine Unlocked*, vol. 9, pp. 200–209, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352914817300795

[9] P. S. Nyasulu, C. Paszko, and N. Mbelle, "A narrative review of the laboratory information system and its role in antimicrobial resistance surveillance in South Africa," *Advances in Microbiology*, 2014. [Online]. Available: http://www.scirp.org/journal/aim

[10] G. Kong and Z. Xiao, "Protecting privacy in a clinical data warehouse," *Health Informatics Journal*, vol. 21, no. 2, pp. 93–106, 2015. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/1460458213504204

[11] E. O. Okpu and O. E. Taylor, "Analysing the integration of AES-256 encryption and HMAC hashing in IoT smart healthcare systems," *Ci-STEM Journal of Digital Technologies and Expert Systems*, vol. 2, no. 1, pp. 18–24, 2025. [Online]. Available: https://cjdtes.ci-stem.org/docs/2025/Jan-Jun-2025/CJDTES020102.pdf

[12] M. K. Bhardwaj and M. Saraswat, "Enhancing security for sensitive medical data in IoT-based healthcare systems," *International Journal of Environmental Sciences*, vol. 11, no. 4s, pp. 1278–1285, 2025. [Online]. Available: https://theaspd.com/index.php/ijes/article/view/1908

[13] P. Mathebeni-Bokwe, "Management of medical records for healthcare service delivery at the Victoria Public Hospital in the Eastern Cape Province: South Africa," Ph.D. dissertation, Univ. of Fort Hare, 2015. [Online]. Available: https://core.ac.uk/download/pdf/186689228.pdf

[14] K. Adegboyega and H. S. E. Musa, "Managing health records in the context of service delivery: issues and challenges," *Covenant Journal of Business and Social Sciences*, vol. 10, no. 2, 2019. [Online]. Available: https://journals.covenantuniversity.edu.ng/index.php/cjbss/article/view/1798

[15] L. P. Luthuli and T. Kalusopa, "The management of medical records in the context of service delivery in the public sector in KwaZulu-Natal, South Africa: the case of Ngwelezana hospital," *South African Journal of Libraries and Information Science*, vol. 83, no. 2, pp. 1–11, 2017. [Online]. Available: https://journals.co.za/doi/abs/10.7553/83-2-1679

[16] M. Al-Dogether, Y. Al-Muallem, M. Househ, B. Saddik, and M. Khalifa, "The impact of automating laboratory request forms on the quality of healthcare services," *Journal of Infection and Public Health*, vol. 9, no. 6, pp. 749–756, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1876034116301411

[17] J. Thomas, "Implementation of a laboratory information system in a simulated laboratory," *American Society for Clinical Laboratory Science*, vol. 30, no. 2, pp. 92–98, 2017. [Online]. Available: https://clsjournal.ascls.org/content/30/2/92.abstract

[18] B. Campbell, G. Linzer, and D. R. Dufour, "Lab Tests Online and consumer understanding of laboratory testing," *Clinica Chimica Acta*, vol. 432, pp. 162–165, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0009898113003768

[19] J. S. Ancker, A. Edwards, S. Nosal, D. Hauser, E. Mauer, R. Kaushal, and the HITEC Investigators, "Effects of workload, work complexity, and repeated alerts on alert fatigue in a clinical decision support system," *BMC Medical Informatics and Decision Making*, vol. 17, no. 1, p. 36, 2017. [Online]. Available: https://link.springer.com/article/10.1186/s12911-017-0430-8

[20] Y. Qiao, O. Asan, and E. Montague, "Factors associated with patient trust in electronic health records used in primary care settings," *Health Policy and Technology*, vol. 4, no. 4, pp.

357–363, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2211883715000593

[21] N. Mathai, M. F. Shiratudin, and F. Sohel, "Electronic health record management: expectations, issues, and challenges," *Journal of Health & Medical Informatics*, vol. 8, no. 3, pp. 1–5, 2017. [Online]. Available: https://pdfs.semanticscholar.org/d08e/8b7df15861750036f8eb28f9d04f2c36ad61.pdf

[22] E. Kim, S. M. Rubinstein, K. T. Nead, A. P. Wojcieszynski, P. E. Gabriel, and J. L. Warner, "The evolving use of electronic health records (EHR) for research," *Seminars in Radiation Oncology*, vol. 29, no. 4, pp. 354–361, Oct. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1053429619300426

[23] P. S. Nyasulu, C. Paszko, and N. Mbelle, "A narrative review of the laboratory information system and its role in antimicrobial resistance surveillance in South Africa," *Advances in Microbiology*, 2014. [Online]. Available: https://research.monash.edu/en/publications/a-narrative-review-of-the-laboratory-information-system-and-its-r

[24] G. Lippi and M. Plebani, "The critical role of laboratory medicine during coronavirus disease 2019 (COVID-19) and other viral outbreaks," *Clinical Chemistry and Laboratory Medicine (CCLM)*, vol. 58, no. 7, pp. 1063–1069, 2020. [Online]. Available: https://www.degruyterbrill.com/document/doi/10.1515/cclm-2020-0240/html

[25] M. M. Yusof and A. Arifin, "Towards an evaluation framework for laboratory information systems," *Journal of Infection and Public Health*, vol. 9, no. 6, pp. 766–773, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1876034116301344

[26] M. Weemaes, S. Martens, L. Cuypers, J. Van Elslande, K. Hoet, J. Welkenhuysen, … and J. Goveia, "Laboratory information system requirements to manage the COVID-19 pandemic: A report from the Belgian national reference testing center," *Journal of the American Medical Informatics Association*, vol. 27, no. 8, pp. 1293–1299, 2020. [Online]. Available: https://academic.oup.com/jamia/article-abstract/27/8/1293/5827002

[27] M. Patterson, "The future of laboratory information systems: user input impacting the development of laboratory information systems," in *Proc. 32nd Int. BCS Human Computer Interaction Conf.*, BCS Learning & Development, 2018. [Online]. Available: https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/HCI2018.95

[28] J. C. Amaechi, V. C. Agbasonu, and S. E. Nwawudu, "Design and implementation of a hospital database management system (HDMS) for medical doctors," *International Journal of Computer Theory and Engineering*, vol. 10, no. 1, 2018. [Online]. Available: http://www.iqytechnicalcollege.com/Hospital%20Data.pdf

[29] Q. Li, "Design and implementation of laboratory information management system for chemical analysis," in *Proc. 2017 5th Int. Conf. Frontiers of Manufacturing Science and Measuring Technology (FMSMT 2017)*. Atlantis Press, 2017. [Online]. Available: https://www.atlantis-press.com/proceedings/fmsmt-17/25875492

[30] K. Srinivasan, G. S. Chauhan, R. Jadon, R. Budda, V. S. T. Gollapalli, and A. Kurunthachalam, "Secure healthcare data storage and access control in cloud computing environments using AES and ECC encryption," *International Journal of Information Technology & Computer Engineering*, vol. 10, no. 3, 2022. [Online]. Available: https://ijitce.org/index.php/ijitce/article/view/967

[31] G. W. W. Mukti and H. Setiawan, "Designing and building secure electronic medical record application by applying AES-256 and RSA digital signature," in *IOP Conf. Series: Materials Science and Engineering*, vol. 852, no. 1, p. 012148, Jul. 2020. IOP Publishing. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/852/1/012148/meta

[32] T. Raharjo and Y. Prayudi, "Securing electronic medical documents using AES and LZMA," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 9, no. 2, pp. 374–384, 2025. [Online]. Available: https://jurnal.iaii.or.id/index.php/RESTI/article/view/6260?utm_source=chatgpt.com

[33] G. Marrivada, "Revolutionizing electronic health records: A technical deep dive into IAM and cybersecurity implementation," *International Journal for Multidisciplinary Research (IJFMR)*, vol. 6, no. 6, 2024. [Online]. Available: https://www.ijfmr.com/research-paper.php?id=33702

[34] J. Reza, K. Y. Ali, M. Rakibuzzaman, M. S. Islam, and M. A. Alam, "Investigating data encryption technologies in securing business information systems," 2023. [Online]. Available: https://wjarr.com/sites/default/files/WJARR-2022-1449.pdf