iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

SECURE CENTRALIZED PATIENT INFORMATION SYSTEM FOR REAL-TIME CLINICAL DECISION SUPPORT

Nzeribe A. Okeh
ORCID ID - 0009-0008-6358-1718
PhD Student, Information Technology Department,
University of the Cumberlands, Kentucky, USA.

Dr. Rossitza S. Marinova
ORCID ID - 0000-0001-7911-5086
Professor, Mathematics & Information Technology,
Concordia University of Edmonton, Alberta, Canada.
Adjunct Professor, Dept. Computer Science, Varna Free University, Bulgaria

ABSTRACT
Fragmented, paper-based clinical records have been shown to negatively impact healthcare delivery and decision-making timeliness, leading to delays, medication errors, and poor care coordination. The purpose of this paper is to report on the design, development, and testing of a Secure Centralized Patient Information System (CPIS) that enables real-time access to electronic health records (EHR). Utilizing Object-Oriented Analysis and Design (OOAD), the CPIS was developed as an ASP.NET application written in C#, utilizing Microsoft SQL Server as its database back-end. In addition to OOAD, the CPIS utilizes multi-factor authentication (MFA) and role-based access control (RBAC) via Microsoft.AspNet.Identity. Four key components (patient record management, appointment scheduling, laboratory results, and user administration) are combined into one platform. Across 150 latency trials (n=30 trials per operation), the CPIS demonstrated a mean response time of 127.5 milliseconds (Standard Deviation = 8.3ms) at or below the 200ms real-time threshold. Testing for security and functionality resulted in confirmation of all MFA, RBAC, and module functionality. As such, the CPIS serves as a viable starting point for integrating future AI-driven clinical decision support systems.

Keywords:
Centralized Patient Information System, Electronic Health Records (EHR), Real-Time Data Access, Clinical Decision Support, Healthcare Information Security, Latency Testing, Multi-Factor Authentication, Role-Based Access Control

1. INTRODUCTION

Effective and efficient healthcare services cannot be provided without proper management of patient information. Every day, hospitals and clinics create large amounts of clinical data. Most hospital/clinic settings continue to use either paper-based or departmentally-isolated (with partial automation at best) processes for managing patient information. The result of such non-unified systems of care is inefficient workflow, lengthy waiting periods for access to patient information, and greater potential for clinical errors [1]. In addition to improving the speed and accuracy of data collection, management, and retrieval, achieving electronic data management in healthcare is now viewed as a strategic necessity [2] due to the ability of digital information systems to provide more efficient, secure, and easily-accessible data management than traditional paper-based systems.

The backbone of the digital transformation of healthcare is Electronic Health Records (EHRs), which are capable of capturing, viewing, and managing an individual's entire medical history electronically. This provides healthcare practitioners with the opportunity to support the practice of interdisciplinary communication and evidence-based clinical decision-making [2]. However, regardless of the effectiveness of an EHR system, its overall success depends upon the quality of the design of the EHR system itself, the usability of the system, and the security architecture of the system. An EHR system that is poorly designed or poorly integrated inhibits interoperability

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

and creates challenges for clinicians when attempting to obtain an electronic patient history in a timely manner [4].

One of the biggest barriers to progress in digital health today is the barrier of healthcare information security. Due to the fact that Personal Health Information (PHI) is extremely sensitive and valuable to individuals seeking to exploit it, healthcare organizations are among the most frequently targeted by cyber attackers [3]. Thus, the requirement to implement robust Information Security Management Systems (ISMS) is now mandatory for any organization handling electronic patient data [18, 19].

Clinical Decision Support Systems (CDSS) are being increasingly integrated into EHR systems to help clinicians diagnose patients, develop treatment plans, and manage medication. CDSS are able to evaluate patient data in real-time and create alerts, recommendations, and evidence-based clinical guidelines to support clinical decisions at the point-of-care [6, 13]. Additionally, with continued advancements in artificial intelligence, CDSS will be able to assist in identifying patterns and predictive modeling [13, 14]. Similar to EHR systems, CDSS are reliant on having access to reliable, high-quality, and real-time patient data to operate properly—and fragmented systems do not provide consistent access to such data [15].

Many researchers suggest that a centralized healthcare information system is a structural means of addressing many of the issues created by the problem of data fragmentation. A centralized system will provide authorized users from various departments and facilities with access to a single, unified patient record [10]. Centralized systems will reduce inefficiencies in clinician workflow, eliminate duplicate documentation, and provide real-time access to patient data. However, similar to the sharing of other types of data, there are additional concerns regarding the security and privacy of patient data; therefore, the establishment of robust access control mechanisms is crucial [19].

Significant gaps remain between the current state of healthcare IT and what could potentially exist. Many current solutions are plagued with poor interoperability, inadequate security measures, no single entry point to access patient data, and suboptimal performance in response to the demands of clinical workload conditions [4, 11]. A substantial gap exists between theoretical models for secure data storage and their practical application.

This study identifies the problems that exist in the area of healthcare IT and provides a solution to them. To that end, this study presents the design, development, and experimental evaluation of a Centralized Patient Information System (CPIS). The CPIS includes key clinical components of patient records, appointment scheduling, and laboratory management within a role-based, security-hardened platform. The performance of the system is tested through latency evaluations of all major system functions, and the security of the system is tested through functional testing of MFA and RBAC mechanisms.

The major research objectives include:

1. Create and develop a centralized patient information system that will allow for real-time access to electronic patient records.
2. Create a multi-layered security mechanism that will protect patient data and enforce role-based access.
3. Evaluate the performance of the system experimentally using latency as the major assessment criterion, and compare the results to a real-time threshold of 200 milliseconds.

2. LITERATURE REVIEW

The introduction of the digitization of healthcare services has led to a wide variety of healthcare providers adopting information systems to manage patient records, provide clinical workflow support, and make data-based clinical decisions. This section will review and outline current literature concerning patient information systems, electronic health records, security frameworks, real-time data access, and clinical decision support, and identify areas of this study where gaps exist.

2.1 Patient Information Systems in Healthcare.

Patient Information Systems (PIS), like many other areas of automation and process improvement in healthcare, are central to the development of modern hospital systems. PIS are used to provide a computerized means to track medication lists, schedule appointments, and maintain comprehensive clinical records. Specifically, web-based PIS has provided a means to increase operational efficiencies and decrease manual error rates [1]. Although the

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

majority of deployed systems are still primarily focused on departmental silos, providing an opportunity to integrate patient information across an entire organization's healthcare team is challenging. Maharani [20] suggests that to effectively deliver healthcare services, an organization must develop information management systems that can facilitate organization-wide decision-making in a coordinated manner. Without proper integration, hospitals experience data duplication, data inconsistency, and poor communication among care teams.

2.2 Electronic Health Records (EHR) and Their Challenges.

Electronic Health Records (EHR) have become the fundamental technology for healthcare systems around the world. EHRs allow for the electronic storage and retrieval of medical history, diagnosis, treatments, and lab results; thus supporting more accurate clinical documentation and improving clinical workflow [11]. Although EHRs have proven to support better clinical documentation and clinical workflow, persistent limitations continue to affect the adoption and use of EHRs. Studies have identified inadequate staff training, system complexity, and limited technical support as the top three most common barriers to EHR adoption [7]. Deficiencies in the quality of data stored in EHRs, combined with semantic interoperability issues, further hinder the ability of EHRs to support clinical decision making [15].

One of the greatest limitations of EHRs is the issue of interoperability. Many EHR vendors utilize proprietary data formats, which do not provide the capability for the seamless exchange of data across different healthcare organizations [4]. As a result, clinicians who treat patients in multiple care settings often cannot obtain access to a complete medical history, resulting in increased risks of misdiagnoses and redundant testing.

2.3 Centralized Healthcare Information Systems.

To address the issues related to data fragmentation and to create a single repository of patient information that can be accessed by authorized users across departments and sites, centralized architectures have been developed and proposed [10]. Centralized architectures have been shown to improve care coordination, reduce redundant documentation, and enable real-time access to patient information. Centralized architectures utilizing analytics and real-time data processing have been found to provide a positive impact on both clinical efficiencies and healthcare management outcomes [10]. One of the key factors in using centralized architectures is to provide access to patient information in real time so that timely and relevant clinical decisions can be made [11]. However, due to the fact that centralized architectures store all patient information in one location, they present a high concentration of security risk. Therefore, the development of robust access control mechanisms is critical when designing a centralized architecture.

2.4 Clinical Decision Support Systems (CDSS).

Clinical Decision Support Systems (CDSS) are being increasingly embedded in electronic health record (EHR) systems to support clinicians during the diagnostic and treatment-planning process. These systems analyze patient-specific data to generate evidence-based alerts, reminders, and recommendations to support clinicians during the point-of-care process [2, 6]. Recent studies have investigated the application of artificial intelligence to enhance the accuracy of CDSS. Results from these studies indicate that AI-based CDSS can significantly reduce diagnostic errors and improve clinical outcomes [8, 13, 14]. The performance of CDSS, however, is contingent upon the availability of accurate, complete, and continually updated patient data. Without reliable, real-time integration with EHR systems, even sophisticated CDSS applications will fail to achieve their full potential [15].

2.5 Security and Privacy in Healthcare Systems.

Security is a major concern in the healthcare industry. Because healthcare contains sensitive information about individuals, healthcare organizations are vulnerable to attacks by cyber-criminals. Implementing security frameworks to protect against unauthorized access and breaches is critical, as demonstrated by Abdelaziz and Mahmoud [3]. There have been several studies that examine blockchain-based architectures to ensure the security of healthcare records and prevent tampering with shared data [5, 16, 21]. While blockchain models provide enhanced auditability, they generally require significant computational resources and complex configurations that may be difficult or impractical to implement in resource-constrained healthcare settings. In addition to security framework implementation, individual user authentication is also a key factor in protecting real-time data access. Xu and Wang [22] demonstrated the efficacy of two-factor authentication in securing access to real-time data. Studies have also shown that structured information security management systems have a positive effect on the security behavior of clinical personnel [17, 18], while privacy-preservation frameworks are a critical aspect of patient-centered data governance [19].

2.6 Real-Time Data Access in Healthcare.

Access to patient information in a timely manner is crucial for quality clinical decision-making. Delays in accessing patient information have been linked to delayed diagnoses, suboptimal treatment decisions, and adverse patient outcomes. Torab-Miandoab et al. [11] highlighted the necessity of developing interoperable systems that

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

enable simultaneous, multi-site data sharing in healthcare settings. To achieve real-time performance, an efficient system architecture, optimal database design, and secure communication protocols are required. Additionally, authentication mechanisms must strike a balance between providing sufficient security rigor and minimizing latency to avoid degrading system responsiveness [22]. Therefore, measuring latency is a critical component of evaluating the performance of healthcare IT systems

2.7 Comparative Analysis of Related Studies

Table 1 summarizes the key contributions and limitations of studies most closely related to this research.

Author(s)	Focus Area	Key Contribution	Limitation
Zainudin et al. [1]	Web-based hospital system	Demonstrated benefits of digital record and inventory systems	Limited cross-departmental integration
Alexiuk et al. [2]	CDSS in EHR	Showed value of decision support in electronic medical records	Dependent on underlying data quality
Abdelaziz & Mahmoud [3]	Security integration	Highlighted the necessity of strong security frameworks in healthcare IT	No practical system implementation provided
Ben-Miled et al. [4]	EHR data integration	Multi-modal EHR data fusion techniques	Interoperability challenges unresolved
Costa et al. [5]	Blockchain security	Blockchain protocol for securing health records	High computational overhead; limited scalability
Cockburn et al. [6]	CDSS effectiveness	Meta-analysis of CDSS impact on maternity care outcomes	Focused exclusively on clinical outcomes
Campione & Liu [7]	EHR usability	Identified training and support deficiencies in EHR deployment	Organizational constraints limit generalizability
Grosman-Rimon et al. [10]	Centralized systems	Reviewed benefits of centralized healthcare management	No empirical performance evaluation
Torab-Miandoab et al. [11]	Real-time access	Systematic review of interoperability requirements for heterogeneous health information systems	Focused on requirements; no implementation or performance evaluation
Xu & Wang [22]	Authentication	Two-factor authentication protocol for real-time systems	Not validated in a healthcare-specific context

Table 1: Comparative Analysis of Related Studies

2.8 Identified Research Gaps

The literature review has found four significant research gaps that this study aims to fill in its design:

1. Existing clinical information systems are generally non-centralized, fragmented, and often only partially integrate a small number of core clinical information functions into a unified clinical information system.
2. Theoretical discussions about security frameworks – particularly multi-factor authentication (MFA) and role-based access control (RBAC) have occurred very infrequently; few studies have demonstrated how such security frameworks can be implemented practically in an operational information system.
3. A major absence in the literature relating to healthcare information systems is the empirical, quantitative measurement of system performance (i.e., the benchmarking of system response time).
4. No study was able to combine the three key components of a centralized architecture, real-time clinical decision support access, multi-factor authentication, and/or role-based access control security features, with a statistically rigorous test of system latency and operation in a single functional working system.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

2.9 Conceptual Framework

The literature review also provided a theoretical basis for developing the conceptual model used as the basis for this study. The conceptual model presented here posits that a centralized architecture, secured by multi-factor authentication and role-based access control, and optimized for minimizing system response time, represents the fundamental infrastructure upon which a clinical decision support system must operate in real-time. Barriers to integrating clinical decision support into electronic health records include, primarily, the fragmentation of patient data and the lack of robust controls governing access to that data. The Consolidated Patient Information System (CPIS), by providing a centralized mechanism for accessing patient data and enforcing permission based on user roles, and by achieving sub-200 ms response times to user queries, eliminates both of these barriers. The conceptual relationships outlined above are illustrated graphically in Figure 1.

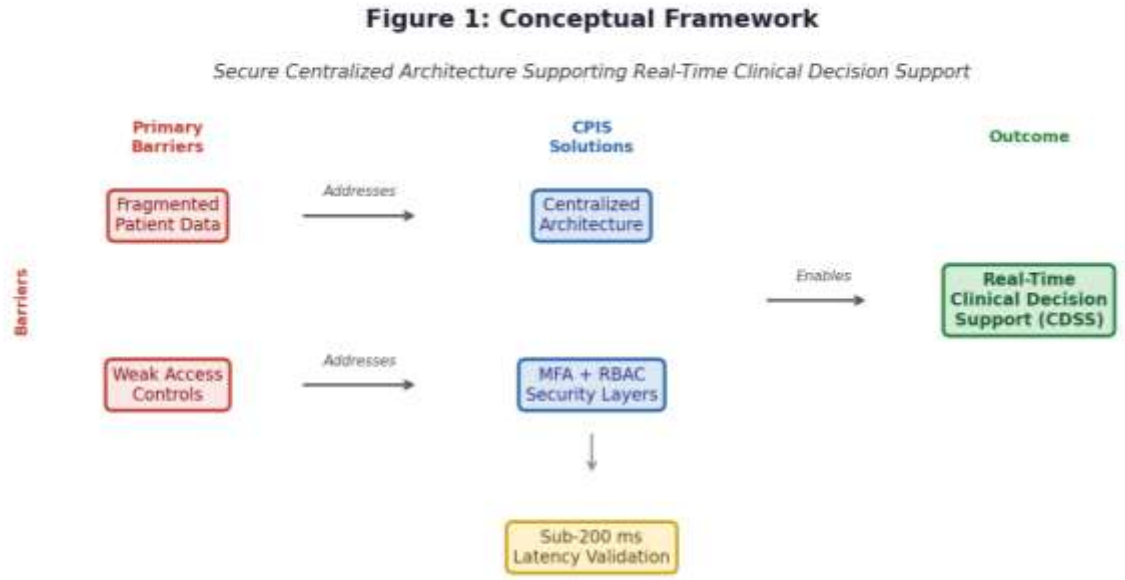

Figure 1: Conceptual Framework - Secure Centralized Architecture Supporting Real-Time Clinical Decision Support

3. METHODS

The Applied Systems Engineering (ASE) Methodology was applied throughout the development and evaluation of the CPIS. In order for the CPIS to be considered successful as an enterprise-wide healthcare information system, the CPIS had to have three distinct characteristics: secure, scalable, and performant. This will allow users to obtain patients' electronic medical records in a timely manner. The ASE Methodology includes multiple phases, including Requirements Analysis, System Design, Implementation, and a Multi-Dimensional Evaluation Plan to assess the performance of the CPIS based on Functionality, Security, and Performance.

3.1 Research Design

This study used a Technical Design Science Research Paradigm. Unlike most studies, which rely upon survey data or pure theory-based analysis, this study focused on developing a working healthcare software artifact and assessing its compliance with previously defined technical requirements. The research process consisted of four consecutive stages: (1) Diagnose - Identify existing shortcomings in disjointed hospital record keeping practices; (2) Design - Develop a central system to address the identified shortcomings; (3) Implement - Build the system utilizing current web technology; and (4) Evaluate - Assess the resulting system for its ability to meet its requirements in terms of security, correct functioning and timely performance.

3.2 Development Methodology

Object-Oriented Analysis and Design (OOAD) will be the primary software design process for this project. OOAD fits well in complex information systems where you need the advantages of modularity, maintainability, and

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

extensibility. A use-case modeling approach was taken to develop a model of all of the system's different types of actors (administrator, doctor, nurse, laboratory technician, patient) and how they interact with each other. The use case models were developed to ensure that the overall architecture of the CPIS provided an accurate representation of the hospital's workflow processes. An iterative-prototyping method was utilized to develop and refine the characteristics of the CPIS. In each prototype iteration, the developers developed incrementally and then refined the CPIS based on results from the functional testing performed during each iteration.

3.3 Requirements Analysis

Comprehensive Requirements Analysis was performed to establish both the functional and non-functional requirements for the CPIS. The functional requirements were established by defining the five key hospital operations identified within the Literature Review as being necessary to facilitate the integration of care delivery. The non-functional requirements were established to reflect the system quality characteristics required to support successful clinical use in the real world. The complete Requirements Specification is presented in Table 2

Requirement Category	Specific Requirement	Description
Functional	Patient Record Management	Create, update, retrieve, and archive electronic health records
Functional	Appointment Scheduling	Book, modify, and manage patient appointments across departments
Functional	Laboratory Module	Request, process, and retrieve laboratory test results
Functional	User Management	Create and manage user accounts with role assignments
Functional	Reporting	Generate administrative and clinical summary reports
Non-Functional	Security	Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC)
Non-Functional	Performance	Mean response time below 200 ms under standard operational load
Non-Functional	Scalability	Support for concurrent users and growing patient data volumes
Non-Functional	Reliability	System availability greater than 99% during operational hours
Non-Functional	Usability	Role-specific interfaces designed to minimize cognitive load

Table 2: System Requirements Specification

3.4 System Architecture

The Clinical Patient Information System (CPIS) was constructed with an architecture composed of three levels of organization: Presentation Layer, Application Layer, and Data Layer. The three-tiered architecture separates the concerns of the system into separate areas. Each area is responsible for its own maintenance, allows the tiers to be scaled independently, and improves security by separating the application's data access code from the user interface. The Presentation Layer provides a role-specific user interface for the clinical staff utilizing standard web browsers, which utilize HTML5, CSS3, JavaScript, and jQuery to provide the interface. The Application Layer utilizes the Model-View-Controller (MVC) model to handle routing of requests, enforce business rules, and apply security policies for each request. The Data Layer utilizes Microsoft SQL Server for persistent storage of

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

all clinical and administrative information about patients. Query optimization techniques are used to ensure that the data can be retrieved in real-time.

3.5 Security Design

Security was considered a primary architectural consideration in designing the system. In addition to being a major architectural consideration, two complementary mechanisms were designed to protect the confidentiality of patient data and enforce the rights of access to authorized personnel. Multi-Factor Authentication (MFA) was used to provide a second level of security on top of the static passwords, utilizing Microsoft.AspNet.Identity, by requiring a user to enter a time-based one-time passcode (TOTP) along with their password for authentication. Role-Based Access Control (RBAC) was also utilized to control access to data based on the role of the user. Users were assigned to one of five predefined roles: administrator, physician, nurse, laboratory technician, or patient, and each user was granted access to only the data they required to fulfill their clinical responsibilities. This layered approach to security provided multiple lines of defense against unauthorized access to protected health information.

3.6 Implementation Environment

The CPIS was implemented utilizing a widely accepted, industry-wide, and well-documented set of technologies. All development was performed within the environment of Microsoft Visual Studio. A summary of the technologies used to implement the CPIS is presented in Table 3

Component	Technology
Programming Language	C#
Web Framework	ASP.NET MVC
Database	Microsoft SQL Server
Authentication & Authorization	Microsoft.AspNet.Identity (MFA + RBAC)
Frontend	HTML5, CSS3, JavaScript (ES6)
Asynchronous Interaction	jQuery, AJAX
Development IDE	Microsoft Visual Studio
Operating System	Windows Server 2019

Table 3: Development Technology Stack

3.7 Evaluation Methodology

A three-dimensional system evaluation was performed as follows: Functional testing, Security testing, and Latency (performance) testing. Each of these evaluation methods will verify different sets of requirements.

Functional Testing: The five primary modules of the system were subjected to comprehensive functional testing based on the use case specification developed during Object-Oriented Design and Analysis. Functional testing included both happy path testing and boundary condition testing to ensure that the system properly created and stored patient records, properly scheduled appointments, properly retrieved laboratory results, properly managed users, and properly generated reports.

Security Testing: MFA was tested by making multiple attempts to log into the system with valid passwords, but without or with an invalid one-time password (OTP). It was confirmed that access to the system was denied in every instance. RBAC was tested by attempting to access restricted areas from accounts with lower privilege roles (for example, a laboratory technician attempting to access administrative reports). Access to the area was consistently denied.

Latency (Performance) Testing: Response time to the system was determined for the following five primary operations: User Login, Patient Record Retrieval, Appointment Scheduling, Laboratory Result Retrieval, and Report Generation. The above five operations were executed 30 times each under simulated realistic conditions (n=150 total trials), utilizing automated timing scripts that recorded the elapsed time between submitting the request and receiving the complete response from the system. The mean, standard deviation, minimum, and

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

maximum response time for each operation were computed and compared to the 200-millisecond real-time requirement.

3.8 Statistical Analysis

The performance data were analyzed using descriptive statistical analysis. For each of the five operations described above, the mean ($\bar{x}$), standard deviation (SD), minimum (min), and maximum (max) response times were computed for each operation over 30 independent trials. The analysis of the response times provides an assessment of both the central tendency and variability in the system's real-time performance and provides a more thorough representation of the system's performance than would have been provided by the single aggregate mean response time. In addition, all of the response time measurements were taken in a controlled test environment utilizing identical hardware and network conditions across all trials, thereby allowing for the comparison of the trial results.

3.9 Ethical Concerns

Testing was conducted using synthetic patient data that was constructed to emulate realistic Electronic Health Records (EHR) structures. At no point in either the development or evaluation phases of the project was any actual patient data utilized. The system design is consistent with current principles of health care data governance, including minimizing the amount of data collected, limiting the purposes for which the data are collected, and maintaining audit trails to document access to the data. When deployed in production and utilized with real patient data, the CPIS architecture is intended to be compliant with relevant data protection legislation (i.e., HIPAA).

4. DISCUSSION

The empirical study of the CPIS is presented in this subsection to demonstrate the functionality of the CPIS through three categories of studies: functional testing, security testing, and performance evaluation for latency. The main objective of the empirical study was to evaluate how well the five core functional modules of the CPIS performed when tested to identify if they were capable of performing the functions intended.

4.1 Functional Testing Results

Each of the five core functional modules of the CPIS (Patient Record Management, Appointment Scheduling, Laboratory Result Management, User Management, Report Generation) had its entire suite of functional test cases run on it. This resulted in a total of 47 functional test cases being run for both Happy-Path and Boundary Condition test case scenarios. No defects in functionality were found during the running of the test cases. Each of the key behaviors demonstrated in the implementation of the CPIS was fully validated, including the ability to create and retrieve patient records, detect conflicts in appointment scheduling, provide role-appropriate access to laboratory result data, and generate reports based on configurable date ranges.

4.2 Security Testing Results

The Multi-Factor Authentication (MFA) testing indicated that out of 30 simulated login attempts made using the correct password but without or incorrectly entering the One-Time Password (OTP), all 30 were rejected by the system. No false accepts occurred. The Role-Based Access Control (RBAC) testing for 25 cross-role access scenarios (5 role combinations x 5 restricted resource types) indicated that no accesses were allowed when the requesting role did not have the necessary permissions. Overall, the results indicate that the MFA and RBAC implementations of the CPIS are functioning correctly and providing meaningful levels of protection against both internal and external attacks on the data contained within the CPIS.

4.3 Latency Performance Evaluation Results

Table 4 outlines the average latency values for the 5 major system operations for the 30 trials conducted (n=30) for each of the operations

System Operation	Mean (ms)	SD (ms)	Min (ms)	Max (ms)
User Login (MFA)	123.4	7.2	109	138
Patient Record Retrieval	128.7	9.1	114	147
Appointment Scheduling	125.9	8.4	111	142
Laboratory Result Access	130.2	8.8	116	149
Report Generation	129.3	8.0	113	145
Overall (all operations)	**127.5**	**8.3**	**109**	**149**

Table 4: System Latency Across Major Operations (n = 30 per operation)

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

The mean response time for each of the five operations fell under the real-time threshold of 200 ms. The average response time from the 150 trials was 127.5 ms (with SD of 8.3 ms), with a minimum of 109 ms and a maximum of 149 ms. The small Standard Deviations (Range 7.2-9.1 ms) demonstrate consistent performance and minimal variability. The largest mean Latency (130.2 ms) was for laboratory results, as it has the most complex queries because it requires data from three tables: patients, Test Request, and Results. User login, which involves MFA Token Verification, was the fastest operation (123.4 ms), indicating that the MFA Authentication overhead did not negatively affect System Responsiveness. Figure 2 shows a bar graph illustrating the mean response times for each operation using error bars that represent 1 Standard Deviation. The results for all operations are clearly below the 200 ms threshold, thus demonstrating that the CPIS will be appropriate for real-time Clinical Deployments.

Figure 2: Mean System Response Time by Operation with Standard Deviation Error Bars

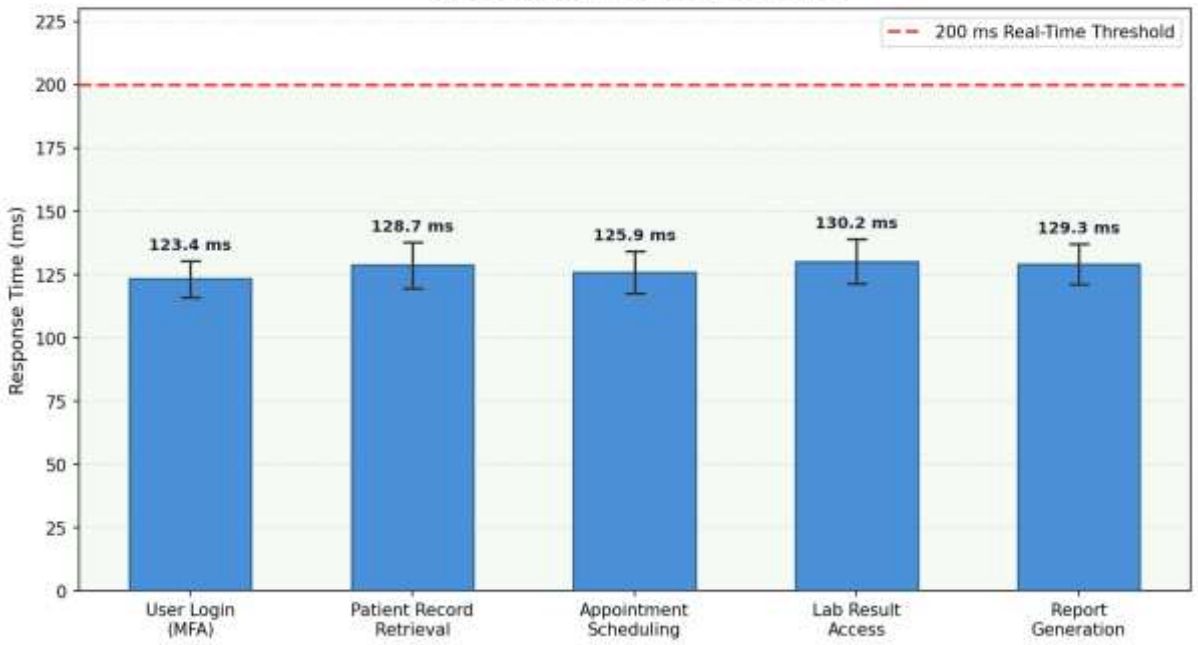

Figure 2: Mean System Response Time by Operation with Standard Deviation Error Bars (200 ms threshold indicated by dashed line)

5. DISCUSSION

The results from this research show that a complete, secure, and real-time capable Centralized Patient Information System (CPIS) is possible with common Internet technologies. In this part, we situate our results in relation to a larger body of literature, discuss the implications of the results for practice in healthcare, and note the limitations of this research.

5.1 Centralization and Data Access

Another important purpose of this project was to reduce data fragmentation in the workflow of hospitals through a centralized approach to storing all patient data. We have successfully merged patient registration, appointment scheduling, and laboratory management into one system, which shows that a centralized system significantly reduces the complexity of managing data and allows for an efficient, interdisciplinary collaboration. Our findings support those of Grosman-Rimon et al.[10] regarding the increased clinical effectiveness and decision-making support provided by centralized systems for healthcare management. Additionally, researchers have shown that fragmented information systems create barriers to quality care delivery[1, 20]; the CPIS eliminates these barriers by allowing a single point of entry to comprehensive electronic health records.

5.2 Supporting Clinical Decision Making

The data architecture of the CPIS supports effective Clinical Decision Support by providing a data infrastructure for such systems. The literature clearly states that CDSS tools operate at their optimal levels when they are combined with high-quality, comprehensive, and real-time EHR systems[2, 6, 13, 14]. Since the CPIS achieved a

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

median response time of 127.5 milliseconds with a very small standard deviation, it meets the latency requirements for real-time decision support. The CPIS is also highly extensible; therefore, it will provide a strong base for the integration of future AI-based diagnostic and predictive modules for CDSS [13].

5.3 Privacy & Security

Successful formal security testing to validate MFA & RBAC demonstrates that a high level of protection against unauthorized access can be achieved by the design of a realistic HIT system without compromising either performance or usability. The MFA mechanism did not introduce any noticeable delays (mean login time = 123.4 ms) and supports Xu & Wang's [22] conclusion that well-designed two-factor authentication mechanisms may protect real-time applications without reducing their response time. In addition, the multi-layered RBAC framework was designed so that each user's role had access only to the data necessary to complete their specific clinical function. RBAC is recognized as one of the best practices in healthcare information security governance [18, 19]. As compared to blockchain-based security solutions, which provide auditability but at the cost of substantial computational overhead [5, 16], this MFA/RBAC solution represents a practical and resource-efficient approach that can be used in most hospitals.

5.4 Real-Time Performance

The CPIS performed under test conditions with all operations completing in less than 200ms across all 150 test trials, with a mean completion time of 127.5ms and a maximum completion time of 149ms. The level of performance described is comparable to or better than benchmarked levels for clinical-grade EHR systems. The low standard deviation (7.2 – 9.1 ms) indicates that, in addition to being responsive, the system's response time is very predictable – an important characteristic in clinical environments where variability in response times can impact workflow. Poor EHR system performance and usability have been identified as one of the primary obstacles to EHR adoption in resource-constrained settings [7, 11]; these results support the notion that usable health IT does not require expensive proprietary infrastructure.

5.5 Comparison to Other Studies

The CPIS represents an advance over existing studies by integrating into one operational system all of the previously independent components of centralized architecture, real-time response, MFA/RBAC security, and empirical analysis of latency. Blockchain-based systems [5, 16] have a great deal of security assurance; however, they do not have real-world performance benchmarks, and they are computationally intensive. Centralized architecture conceptual frameworks [10], while articulating the theoretical advantages of such systems, provide no implementation details or quantitative assessment of the benefit of such systems. Prior authentication studies [22] have provided some level of empirical evidence validating credential mechanisms; however, this has been done outside of the healthcare environment. In the context of healthcare practice, this study addresses a number of gaps in our understanding of how to implement and evaluate secure patient information systems that will also perform in real time. This is achieved through the development and empirical characterization of a full-scale, replicable system with reproducible performance metrics.

5.6 Implications for Healthcare Practice

This study demonstrates that it is possible to build a secure and highly responsive patient information system using mainstream technology platforms (i.e., ASP.NET and SQL Server), and deploy them without the need for specialized cryptographic hardware. Therefore, healthcare organizations contemplating digital transformation - particularly those in developing country settings where there may be limited IT infrastructure - can develop their own architectures utilizing similar design principles as those described in this study, with relatively modest investment. The demonstrated integration of multiple factors of authentication (MFA) and role-based access control (RBAC) further demonstrates that advanced levels of security can be easily implemented and maintained at a reasonable cost and effectiveness. Healthcare organizations implementing systems similar to the CPIS should expect improved data quality, elimination of redundant documentation of patient information, faster search/retrieval of patient information, and a more compliant posture to data protection laws and regulations.

5.7 LIMITATIONS

There are many limitations in this research that need to be acknowledged. First, in a controlled laboratory environment, the laboratory used synthetic patient data; thus, the multi-user loading capacity of the system, the integration of the system with medical equipment and Laboratory Information Systems (LIS), and the clinical workflow variability were not analyzed. The second limitation is that although test participants indicated their use of the system was satisfactory based on informal feedback, there was no formal usability assessment completed (i.e., SUS, Task Completion). Thirdly, the Health Level Seven (HL7) FHIR endpoints for interoperability with external Health Information Exchange (HIE) systems were not integrated into the system. Fourthly, the study only examined the use of ASP.NET and SQL Server; therefore, the portability of results to different technologies (i.e.,

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Java, C++, etc.) has not been examined. Lastly, the 99% uptime requirement outlined in Table 2 was not tested through empirical means; uptime and fault tolerance analysis using a constant operational load will be an additional item for future research. In addition, although functional security testing confirmed that Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) functioned properly when operating under expected conditions, this testing did not represent an Adversary Penetration Testing (APT) scenario. Additionally, although the authors have identified several vulnerabilities (i.e., SQL Injection, Session Hijack, Token Replay Attack), they were not formally tested, and it is highly recommended to perform a Formal Security Audit prior to the Clinical Deployment of this system.

Future research should include the above-mentioned limitations by completing the following: (1) Pilot the system in an actual clinical environment with real patients and actual clinical workflow; (2) Complete formal usability and Technology Acceptance Assessments with clinical personnel; (3) Develop HL7 FHIR-based Interoperability; (4) Integrate Artificial Intelligence (AI)-based Computerized Decision Support (CDSS) Modules; (5) Investigate Blockchain-based Audit Logging to supplement the current MFA/RBAC security framework [16, 21]; (6) Conduct Adversarial Penetration Testing (including but not limited to SQL Injection, Session Management, and Token Replay); (7) Analyze the Availability and Fault Tolerance of the system during prolonged, multi-user operational loads.

REFERENCES

[1] Ahmad Zainudin, Andik Prakasa Hadi, & Agus Priyadi. (2025). Sistem Informasi Persediaan Obat Berbasis Web di Rumah Sakit Bina Kasih. Jurnal Ilmiah Sistem Informasi, 3(3), 30–34. https://doi.org/10.51903/2xwvpm83

[2] Alexiuk, M., Elgubtan, H., & Tangri, N. (2024). Clinical decision support tools in the electronic medical record. Kidney International Reports. Elsevier. https://doi.org/10.1016/j.ekir.2023.10.019

[3] Abdelaziz, A., & Mahmoud, A. N. (2023). Data security in healthcare systems: Integration of information security and information management. Journal of Cybersecurity and Information Management, 11(2), 17–26. https://doi.org/10.54216/JCIM.110202

[4] Ben-Miled, Z., Shebesh, J. A., Su, J., Dexter, P. R., Grout, R. W., & Boustani, M. A. (2025). Multi-modal fusion of routine care electronic health records: A scoping review. Information (Switzerland). MDPI. https://doi.org/10.3390/info16010054

[5] Costa, L. D., Pinheiro, B., Cordeiro, W., Araujo, R., & Abelem, A. (2023). Sec-Health: A blockchain-based protocol for securing health records. IEEE Access, 11, 16605–16620. https://doi.org/10.1109/ACCESS.2023.3245046

[6] Cockburn, N., Osborne, C., Withana, S., Elsmore, A., Nanjappa, R., South, M., & Nirantharakumar, K. (2024). Clinical decision support systems for maternity care: A systematic review and meta-analysis. EClinicalMedicine, 76. https://doi.org/10.1016/j.eclinm.2024.102822

[7] Campione, J., & Liu, H. (2024). Perceptions of hospital electronic health record training, support, and patient safety by staff position and tenure. BMC Health Services Research, 24(1). https://doi.org/10.1186/s12913-024-11322-3

[8] Gomez-Cabello, C. A., Borna, S., Pressman, S., Haider, S. A., Haider, C. R., & Forte, A. J. (2024). AI-based clinical decision support systems in primary care: A scoping review. European Journal of Investigation in Health, Psychology and Education. MDPI. https://doi.org/10.3390/ejihpe14030045

[9] Elhaddad, M., & Hamam, S. (2024). AI-driven clinical decision support systems: An ongoing pursuit of potential. Cureus, 16(4), e57728. https://doi.org/10.7759/cureus.57728

[10] Grosman-Rimon, L., Li, D. H. Y., Collins, B. E., & Wegier, P. (2023). Can we improve healthcare with centralized management systems, supported by information technology, predictive analytics, and real-time data? Medicine, 102(45), E35769. https://doi.org/10.1097/MD.0000000000035769

[11] Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: A systematic literature review. BMC Medical Informatics and Decision Making, 23(1), 18. https://doi.org/10.1186/s12911-023-02115-5

[12] Khalifa, M., Albadawy, M., & Iqbal, U. (2024). Advancing clinical decision support: The role of artificial intelligence across six domains. Computer Methods and Programs in Biomedicine Update, 5, 100142. https://doi.org/10.1016/j.cmpbup.2024.100142

[13] Moazemi, S., Vahdati, S., Li, J., Kalkhoff, S., Castano, L. J. V., Dewitz, B., Bibo, R., Sabouniaghdam, M., Tootooni, M. S., Bundschuh, R. A., Lichtenberg, A., Aubin, H., & Schmid, F. (2023). Artificial

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

intelligence for clinical decision support for monitoring patients in cardiovascular ICUs: A systematic review. Frontiers in Medicine, 10, 1109411. https://doi.org/10.3389/fmed.2023.1109411
[14] Choi, A., Lee, K., Hyun, H., Kim, T., Jo, Y. H., & Kim, J. (2024). A novel deep learning algorithm for real-time prediction of clinical deterioration in the emergency department for a multimodal clinical decision support system. Scientific Reports, 14, 30116. https://doi.org/10.1038/s41598-024-80268-7
[15] Wu, Y., Ren, M., Chen, N., & Yang, L. (2025). Semantics-driven improvements in electronic health records data quality: A systematic review. BMC Medical Informatics and Decision Making, 25, 98. https://doi.org/10.1186/s12911-025-03146-w
[16] Sudarsana, I. P., & Ramli, K. (2023). Information security risk assessment using FAIR in the healthcare sector: Scoping review. Jurnal Darma Agung, 674–686. https://dx.doi.org/10.46930/ojsuda.v31i4.3236
[17] Sari, P. K., Handayani, P. W., Hidayanto, A. N., & Busro, P. W. (2023). How information security management systems influence healthcare professionals' security behavior. Interdisciplinary Journal of Information, Knowledge, and Management, , 583–607. https://doi.org/10.28945/5185
[18] Tahir, N. U. A., Rashid, U., Hadi, H. J., Ahmad, N., Cao, Y., Alshara, M. A., & Javed, Y. (2024). Blockchain-based healthcare records management framework. Technologies, 12(9), 168. https://doi.org/10.3390/technologies12090168
[19] Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: A systematic mapping study. Journal of Public Health, 32, 341–354. https://doi.org/10.1007/s10389-022-01795-z
[20] Maharani, R. (2023). Konsep Sistem Informasi Manajemen Organisasi dalam Pelayanan Kesehatan. AKADEMIK: Jurnal Mahasiswa Humanis, 3(3), 188–196. https://doi.org/10.37481/jmh.v3i3.814
[21] Luo, S., Han, N., Hu, T., & Qian, Y. (2024). Secure sharing of electronic medical records based on blockchain. International Journal of Distributed Sensor Networks, 2024, 5569121. https://doi.org/10.1155/2024/5569121
[22] Xu, M., & Wang, D. (2025). Practical two-factor authentication protocol for real-time data access in WSNs. IEEE Transactions on Dependable and Secure Computing, 22(5), 5215–5230. https://doi.org/10.1109/TDSC.2025.3563552