ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV028

UAClinic: Design and Development of a Secure Healthcare Appointment System Employing Advanced Encryption Standard (AES) for the University of the Assumption

Ronian E. Gulles; Charlene Lugtu; Glenn P. Peña
University of the Assumption

Abstract
Traditional university clinic appointment systems often rely on manual processes, leading to scheduling conflicts, record inaccuracies, and compromised data security. To address these challenges, this study developed UAClinic, a secure healthcare appointment system designed specifically for the University of the Assumption. Using the Agile Software Development Methodology, the system was engineered using a modern technology stack consisting of React Native for cross-platform interface delivery, Django REST Framework for backend business logic, and PostgreSQL for robust relational data persistence. The foundational core of the platform is the integration of the Advanced Encryption Standard (AES) via Fernet symmetric cryptography, ensuring end-to-end confidentiality of sensitive electronic patient health records by transforming plain medical records, consultation notes, and visit histories into unreadable ciphertext. Technical verification and software quality evaluation based on the ISO/IEC 25010 model and the System Usability Scale (SUS) confirmed that the AES implementation provides enterprise-grade data protection without compromising real-time system responsiveness, achieving an overall grand mean of 3.31 ("Very High"). The results demonstrate that UAClinic successfully streamlines the appointment lifecycle, mitigates operational bottlenecks, and establishes a secure, privacy-centric digital framework for institutional healthcare management.

Keywords: *AES Encryption, Clinic Appointment System, Healthcare Scheduling, Healthcare Information Systems, JWT Authentication, Role-Based Access Control (RBAC).*

I. INTRODUCTION

1.1 Background of the Study

The digital transformation of modern healthcare services has revolutionized patient record management and appointment workflows. However, educational institutions—such as the University of the Assumption—frequently continue to rely on manual, paper-based clinic procedures. Traditional operations are plagued by operational deficiencies, including scheduling conflicts, prolonged student wait times, delayed communication, and discrepancies in physical medical files.

Beyond routine logistical challenges, contemporary healthcare informatics prioritizes the protection of highly sensitive medical and personal data. Student and faculty health profiles, consultation notes, diagnoses, and medical histories are inherently confidential. In an interconnected environment, digital health data storage and transmission must be safeguarded against unauthorized interception, privilege escalation, and data breaches to preserve institutional integrity and patient trust (Gupta & Denton, 2008; Chiu et al., 2020).

To overcome these vulnerabilities, this research integrates the Advanced Encryption Standard (AES)—a globally recognized, symmetric-key cryptographic cipher renowned for high-speed computational efficiency and impenetrable mathematical security (Daemen & Rijmen, 2020). AES acts as an active defensive barrier, converting medical consultation notes and patient data into encrypted ciphertext prior to database persistence. Consequently, unauthorized parties or compromised database storage layers cannot extract identifiable clinical records without valid cryptographic keys (Khozaimi et al., 2020).

UAClinic bridges the gap between healthcare accessibility and data privacy by establishing an AES-reinforced, multi-role digital ecosystem. Integrated with JSON Web Token (JWT) stateless authentication and Role-Based Access Control (RBAC), the platform delivers automated, role-segregated workflows for students, clinic physicians, and administrative personnel.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV028

1.2 Objectives of the Study

General Objective: To design, develop, and evaluate a secure, efficient clinic appointment system for the University of the Assumption that streamlines scheduling and safeguards sensitive medical records using Advanced Encryption Standard (AES) cryptography.

Specific Objectives:

1. To design and implement a digital appointment scheduling platform accessible to students and healthcare staff.
2. To embed AES symmetric encryption for the secure storage and transmission of confidential patient health information.
3. To enforce rigorous authentication and authorization layers utilizing JSON Web Tokens (JWT) and Role-Based Access Control (RBAC).
4. To facilitate real-time appointment tracking, queue status monitoring, and schedule adjustments.
5. To optimize university clinic operations through automated, paperless record management.

II. LITERATURE REVIEW

Recent advances in health informatics highlight the urgent necessity of transitioning institutional medical services from paper-bound paradigms to centralized Electronic Medical Record (EMR) and appointment scheduling systems. Gupta and Denton (2008) emphasize that healthcare appointment delays and schedule mismatches directly degrade user satisfaction and operational productivity. Automating appointment scheduling minimizes queue bottlenecks and eliminates human errors inherent in physical logbooks.

However, the digitalization of health records introduces significant privacy risks. Chiu, Liu, and Tu (2020) noted that user adoption and trust in online clinic systems depend fundamentally on system reliability, interface usability, and data security guarantees. Medical information systems demand stringent confidentiality controls, as unauthorized disclosure of medical diagnostics infringes upon statutory privacy regulations and patient rights.

To safeguard sensitive health repositories, cryptographic mechanisms are essential. Advanced Encryption Standard (AES), established by the National Institute of Standards and Technology (NIST) and analyzed by Daemen and Rijmen (2020), represents the international benchmark for symmetric block ciphers. Mulyono et al. (2021) demonstrated that implementing AES within electronic medical record architectures ensures high data integrity and confidentiality with negligible latency overhead. By combining AES encryption at rest with JSON Web Token (JWT) tokenization and Role-Based Access Control (RBAC), modern distributed web applications can reliably isolate patient records, verify practitioner credentials, and prevent unauthorized database inspection.

III. RESEARCH METHODOLOGY

3.1 Conceptual Framework

The system was architected using the Input-Process-Output (IPO) framework:
Input: System functional requirements, hardware/software specifications, user and patient personal information, and clinical security compliance parameters.

Process: Agile development sprints, requirement analysis, UI/UX prototyping, full-stack software development (React Native, Django REST, PostgreSQL), AES cryptographic module implementation, JWT/RBAC security configuration, and multi-tier testing.

Output: UAClinic: A fully functional, AES-secured healthcare appointment and clinical record management system for the University of the Assumption.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV028

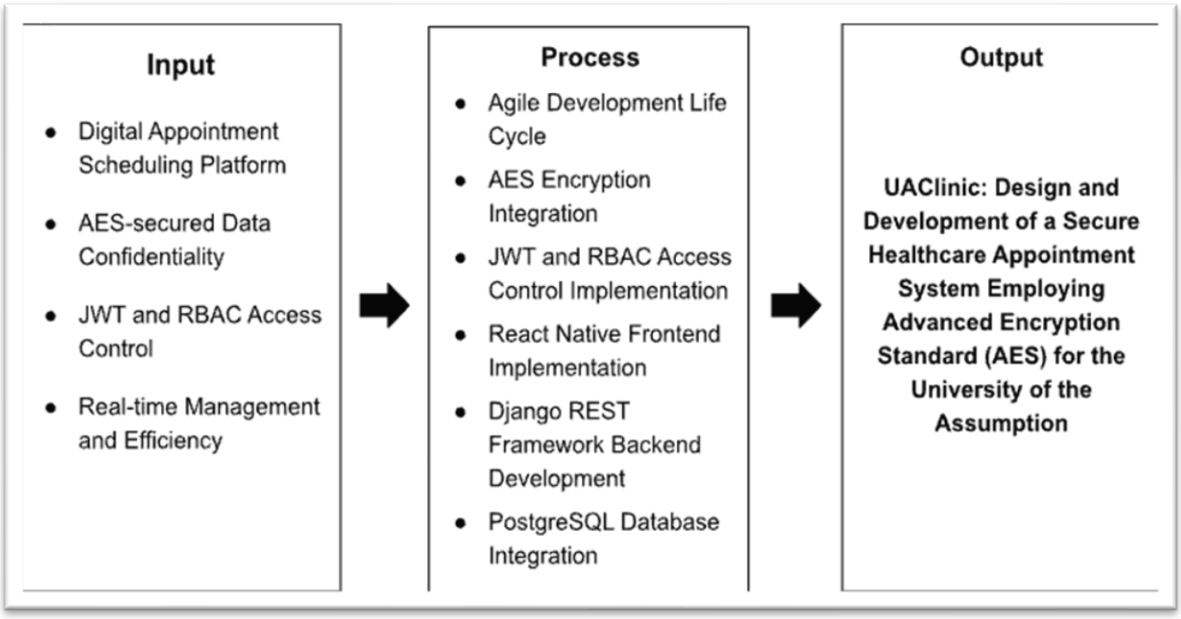


Fig. 1. Conceptual Framework

3.2 Software Development Lifecycle

The project employed the Agile Development Methodology. Because cryptographic components require iterative testing, Agile enabled continuous cycles of:

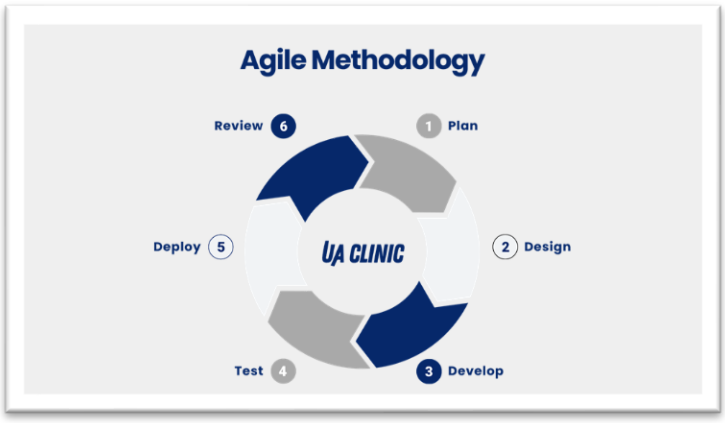


Fig. 2. Agile Development Model

Each two-week sprint delivered testable modules, allowing security and user interface refinements based on direct practitioner feedback.

3.3 System Implementation & Architecture

Frontend Client: Developed with React Native, ensuring a uniform, responsive user experience across desktop and mobile devices.

Backend Services: Powered by Django REST Framework (Python), supplying robust API endpoints, ORM data abstraction, and administrative security.

Database: Managed using PostgreSQL relational database system for ACID-compliant, secure data persistence.
Cryptographic Core: Implemented via Python's cryptography.fernet module, executing 128-bit AES in CBC mode with PKCS7 padding and HMAC-SHA256 authentication:

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV028



```python
from cryptography.fernet import Fernet
import os
from dotenv import load_dotenv

# Load environment variables (FERNET key)
load_dotenv()

# Initialize encryption key and Fernet instance
KEY = os.getenv("FERNET_KEY")
fernet = Fernet(KEY)

def encrypt(text):
    """Encrypts plain text into secure token"""
    if not text:
        return ""
    return fernet.encrypt(text.encode()).decode()

def decrypt(token):
    """Decrypts secure token back to plain text"""
    if not token:
        return ""
    try:
        return fernet.decrypt(token.encode()).decode()
    except Exception:
        return "[Decryption Error]"
```

Fig. 3. AES Algorithm Code

3.4 Research Participants & Setting

The study was conducted at the University of the Assumption, City of San Fernando, Pampanga, Philippines. Participants comprised registered university students seeking medical consultations, university clinic physicians, and healthcare administrative staff. Strict role-based segregation ensured that only authorized institutional users could access system interfaces.

3.5 Evaluation Instruments & Data Analysis

System evaluation was structured using the ISO/IEC 25010 Software Quality Model alongside the System Usability Scale (SUS). Technical verification evaluated AES cryptographic throughput, encryption latency, and database query responsiveness. Survey feedback from students, medical staff, and administrators was statistically evaluated using descriptive statistics (grand means).

IV. RESULTS AND DISCUSSION

4.1 Functional Modules and User Interfaces

The resulting platform encapsulates the end-to-end appointment and clinical management workflow across dedicated stakeholder views:

1. Secure Authentication Module: Supports institutional single-sign-on ("Continue with UA Email") and password authentication, establishing a JWT token session.

2. Registration Module: Captures structured student demographic and academic profiles (Course, Date of Birth, Gender, Emergency Contact).

3. Student/Patient Dashboard: Central navigation hub displaying upcoming appointment status cards and an interactive appointment history filterable by status (Completed, Rejected, Cancelled, Expired).

4. Physician Dashboard & Schedule Manager: Provides doctors with real-time operational metrics (Today's Total, Pending, Completed, Remaining), a rapid approval queue ("Needs Your Approval"), and calendar tables to approve or decline consultation requests.

5. System Administration & Account Management: Supplies comprehensive oversight over clinic operations, real-time audit logs, directory searching, and user role management (Patient, Doctor, Admin).

4.2 Cryptographic Verification

Technical verification confirmed that sensitive patient fields—such as consultation notes, vital signs, and past medical history—are fully transformed into base64 ciphertext tokens prior to disk persistence in PostgreSQL. The encryption and decryption overhead was measured to be negligible, maintaining instantaneous sub-second response times across the React Native client.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV028

4.3 Software Quality Evaluation (ISO/IEC 25010)

The system was evaluated across seven quality dimensions. Table 1 summarizes the perceived usefulness and technical performance scores:

Table 1 Summary of Perceived Usefulness

Characteristics	Grand Mean	Verbal Interpretation
Functional Suitability	3.13	High
Performance Efficiency	3.4	Very High
Compatibility	3.6	Very High
Interaction Capability	3.52	Very High
Maintainability	2.96	High
Flexibility	3.4	Very High
Safety	3.52	Very High
Final Grand Mean	**3.31**	**Very High**

The evaluation demonstrates that UAClinic delivers exceptional reliability, high compatibility across heterogeneous devices, and robust data protection, validating its practical readiness for full institutional deployment.

V. CONCLUSION

5.1 Conclusion

The development and technical validation of UAClinic successfully addresses the operational bottlenecks, scheduling errors, and data security vulnerabilities inherent in traditional paper-based clinic procedures. By coupling modern web engineering (React Native, Django REST, PostgreSQL) with robust symmetric cryptography (AES-Fernet) and access control (JWT/RBAC), the platform ensures complete confidentiality for sensitive student health records while providing a seamless appointment scheduling experience. The high overall evaluation score (3.31 Grand Mean) confirms that digital healthcare management can achieve superior administrative efficiency without compromising patient data privacy.

5.2 Recommendations

1. Automated Multi-Channel Notifications: Implement automated SMS and institutional email push notifications to deliver real-time booking confirmations and appointment reminders.

2. Clinical Data Analytics Dashboard: Incorporate predictive visualization tools for clinic administrators to analyze disease trends, peak visit hours, and population health patterns.

3. Full Electronic Medical Record (EMR) Integration: Expand system capabilities into a comprehensive campus EMR platform supporting digital prescription writing, laboratory diagnostic uploads, and physician consultation notes.

4. Continuous Security Audits: Institute recurring penetration testing and cryptographic key rotation protocols to ensure ongoing resilience against evolving cyber threats.

REFERENCES

[1]. Chiu, H., Liu, G., & Tu, Y. (2020). Determinants of trust in health information technology: An empirical investigation in the context of an online clinic appointment system. International Journal of Human-Computer Interaction, 36(12), 1095–1109.
[2]. Daemen, J., & Rijmen, V. (2020). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.
[3]. Gupta, D., & Denton, B. (2008). Appointment scheduling in health care: Challenges and opportunities. IIE Transactions, 40(9), 800–819.
[4]. Khozaimi, A., et al. (2020). Implementation of Advanced Encryption Standard (AES) for secure communication and storage of sensitive data in web-based applications. Journal of Computer Security and Information Systems, 11(2), 45–53.
[5]. Mulyono, A., et al. (2021). Securing the electronic medical record by implementing Advanced Encryption Standard (AES) on the information system of a health service place. Journal of Physics: Conference Series, 1823(1), 012014.