IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

MedVault: A Privacy-First Web Application for Secure and Patient-Controlled Medical History Management

Mayank Sinha[1], Vedant Kanojia[2], Mohit Kalantri[3]
Department of Computer Science Engineering[1,2,3]
MIT ADT University, Pune, India

Abstract: *The digitalization of healthcare has improved efficiency but also introduced critical concerns regarding the privacy and control of patient data. Traditional systems often lack adequate security measures, centralized privacy controls, and patient-centric authorization. This paper presents **MedVault**, a privacy-first web application for secure medical history management. MedVault enables patients to securely store and control access to their medical records using end-to-end encryption, OTP-based authentication, and role-based access control. Doctors can request access, but only upon explicit patient approval, ensuring transparency through audit logs and secure cloud storage.*

Keywords: Medical data privacy, role-based access, end-to-end encryption, secure health records, patient data control

I. INTRODUCTION

In recent years, the global healthcare system has increasingly embraced digital transformation to streamline medical processes and improve access to care. Despite these advancements, the protection of sensitive patient data has not kept pace. Many existing systems are prone to data breaches, unauthorized access, and misuse of personal health information. The introduction of MedVault addresses these growing challenges by offering a solution that enhances both data security and user autonomy. The platform aims to create a secure bridge between patients and healthcare providers, empowering patients with complete control over their medical histories while maintaining rapid access for clinicians when needed.

II. OBJECTIVES

The primary goals of the MedVault system include:

- Developing a platform that enables secure, encrypted storage of medical records.
- Facilitating patient-controlled access to personal health information.
- Ensuring all data transactions are logged and auditable for transparency.
- Providing OTP-based authentication to prevent unauthorized access.
- Implementing role-based access to distinguish privileges between doctors, patients, and admins.
- Improving trust in the healthcare system by reinforcing ethical data management practices.

III. OVERVIEW OF EXISTING APPLICATIONS

Several digital solutions exist for managing health records, but they exhibit substantial shortcomings:

- **Microsoft HealthVault**: Discontinued due to limited user engagement, lacked robust encryption and control mechanisms.
- **Apple Health Records**: Secure, but only available on iOS; does not offer doctor approval workflows.
- **Google Fit / Samsung Health**: Primarily designed for fitness tracking, not medical-grade record management.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

- **EMR Systems (EPIC, Cerner)**: Institutional tools with limited patient authority and no support for external sharing or real-time access control.

These solutions either neglect user control or are institution-centric, thus failing to provide the transparency and flexibility that MedVault offers.

IV. USER NEEDS AND GAPS IN CURRENT SOLUTIONS

Patients need a centralized, easy-to-use platform to manage their health records and determine who has access to their data. Existing systems tend to favor institutional access over patient control, which diminishes trust and patient empowerment. Furthermore, current systems often lack comprehensive audit trails, which can lead to untraceable data access and potential misuse. Consistent implementation of strong encryption and role-based access control is also missing across many platforms, creating significant gaps in user data security and transparency.

User needs have evolved beyond basic data access. Patients now expect:

- **Control**: Ability to approve/deny access on a per-request basis.
- **Security**: Advanced encryption and secure authentication methods.
- **Transparency**: Real-time alerts and full audit logs for access history.
- **Accessibility**: Cross-platform availability and cloud-based storage.

Current solutions do not meet all these needs simultaneously. MedVault bridges this gap by combining these features into one coherent and user-friendly platform.

V. RATIONALE FOR THE RESEARCH

Healthcare is inherently personal, and thus, patient trust is paramount. A breach of medical data can lead to stigma, discrimination, and compromised treatment. Traditional EMR systems prioritize clinical utility over patient empowerment. This research is grounded in the principle that patients should be the primary custodians of their data. MedVault is not only a technical innovation but a step toward ethical reform in digital healthcare. It reinforces the argument for decentralized, patient-first data models, leveraging technology to restore confidence in health data management.

VI. METHODOLOGY

6.1 Design Approach

- **Agile Development**: Modular, feedback-driven iterations to incorporate real-time user input.
- **Frontend**: Developed in ReactJS to ensure responsiveness, modularity, and reusability.
- **Backend**: Built using Node.js and Express.js for high performance and asynchronous handling.
- **Database**: MongoDB used for its flexible document structure and strong encryption support.
- **Security Layers**: Integrated AES-256 for record encryption and HTTPS for secure transport.
- **Authentication**: OTP-based login using Twilio/Email API to prevent password-related vulnerabilities.

6.2 Features Developed

- **OTP-based Login System**: Replaces traditional password systems, reducing brute-force vulnerabilities.
- **Patient-Controlled Authorization**: Doctors send requests; patients must approve via dashboard.
- **Audit Logs**: Immutable logs showing who accessed what and when.
- **Role-Based Access**: Distinct dashboards and permissions for doctors, patients, and admins.
- **Cloud Storage Integration**: Using AWS S3 or Firebase Storage to hold encrypted records.
- **Encryption Layer**: Files encrypted client-side before upload, decrypted only upon access with patient consent.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

6.3 Evaluation Metrics

Security:

- AES-256 encryption tested with standard cryptographic benchmarks.
- OTP success rate above 98% in internal simulations.

Usability:

- Survey of 50 test users using SUS (System Usability Scale) yielded a score of 85/100.

Performance:

- Access request round-trip averaged 2.7 seconds.
- Dashboard load time under 1 second for 90% of users.

Transparency:

- 100% of access logs traceable and readable.
- Zero unauthorized accesses recorded during stress testing.

VII. KEY FEATURES AND FUNCTIONALITIES

- **OTP Authentication**: Reduces risks of password leaks and improves security.
- **User Dashboard**: Central hub for managing records, requests, approvals, and notifications.
- **Access Requests**: Doctors send requests with specific justification.
- **Encrypted Cloud Storage**: Files stored in encrypted form on the cloud.
- **Audit Trails**: Shows date, time, user ID, and record accessed.
- **Role-Based UI**: Simplified views for doctors (view patient files), patients (approve requests), and admins (monitor activity).
- **Cross-Platform Support**: Responsive design for desktop and mobile.
- **Data Sharing Logs**: Patients can review past sharing activity to identify trends or suspicious behavior.

VIII. RESULTS AND ANALYSIS

Security Performance:

- No breaches in ethical hacking simulations.
- All audit trails validated using hash-checking.

User Experience:

- 92% satisfaction in prototype testing phase.
- Most appreciated feature: Full control over access approvals.

Operational Metrics:

- 80% reduction in unauthorized access attempts compared to traditional EMRs (simulated tests).
- High adoption willingness among test users, with 70% saying they would recommend the app to their healthcare providers.

Doctor Feedback:

- Reported faster access when patients were responsive.
- Requested automated reminders for pending approvals (noted for future versions).

IX. CONCLUSION

MedVault represents a shift in the paradigm of digital health data management, moving from institutional authority to patient sovereignty. It effectively combines modern encryption, transparent audit systems, and granular access control to protect user data while ensuring clinical utility. This research validates that it is both feasible and beneficial to place control of health records in the hands of the patient. Future work will focus on AI-based decision support tools, HL7/FHIR integration for EMR interoperability, and mobile apps for broader reach and convenience.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

REFERENCES

[1]. HIPAA Journal. "What is HIPAA Compliance?" https://www.hipaajournal.com/
[2]. Apple Inc. "Apple Health Records." https://www.apple.com/healthcare/health-records/
[3]. Google Health. "Bringing together health data." https://health.google/
[4]. J. Walker et al., "The Value of Health Care Information Exchange," *Health Affairs*, 2005.
[5]. D. McGraw et al., "Privacy as an enabler, not an impediment," *Health Affairs*, 2009.
[6]. Schneier, Bruce. *Applied Cryptography*. Wiley, 2015.
[7]. OWASP. "Secure Coding Practices." https://owasp.org/
[8]. NIST. "Guidelines for Health IT Security." https://csrc.nist.gov/
[9]. HL7 International. "FHIR Overview." https://www.hl7.org/fhir/
[10]. Kumar, A. & Laxmi, V. "Secure Medical Data Sharing Using Blockchain," *IEEE Access*, 2020.
[11]. M. Ali et al., "Secure Sharing of EHR using Attribute-Based Encryption," *Computers in Biology and Medicine*, 2019.
[12]. IBM Cloud. "Data Security Best Practices." https://www.ibm.com/cloud/blog/data-security-best-practices
[13]. Amazon Web Services. "HIPAA Compliance on AWS." https://aws.amazon.com/compliance/hipaa-compliance/
[14]. S. Ruj et al., "Privacy in Healthcare Data Sharing," *IEEE Internet Computing*, 2018.
[15]. S. Bhattacharya et al., "Digital Trust in e-Health," *Journal of Medical Internet Research*, 2021