SCCFS: Filing System for St. Clare College of Caloocan Registrar

Wenelyn M. Almonte[1], John Michael D. Catamin[1], Joshua Andre B. Cervantes[1], Rolan Jr. I. Chan[1], Geo D. Gutierrez[1], Jude Gabriel L. Salinas[1], Russel B. Sigales[1], Marielle Nicole G. Silvestre[1], Mohammad-Rashlanie M. Unda[1], Jeanethjoy D. Naturales[2]

[1]Institute of Computer Studies, St. Clare College of Caloocan, Caloocan City, Philippines

[2]Professor, Institute of Computer Studies, St. Clare College of Caloocan, Caloocan City, Philippines

DOI: https://doi.org/10.51584/IJRIAS.2026.11050106

Received: 06 May 2026; Accepted: 12 May 2026; Published: 03 June 2026

ABSTRACT

The academic registrar's office manages sensitive student records that require long-term confidentiality, integrity, and rapid accessibility. Traditional manual filing systems are prone to misfiling, physical degradation, and inefficient retrieval, while cloud-based alternatives introduce recurring costs, internet dependency, and data privacy concerns. This study presents the development of an offline-first, Electron-based desktop filing system tailored for the St. Clare College of Caloocan Registrar. The system integrates AES-256-GCM encryption for data-at-rest, SQLite-based metadata indexing for fast offline search, and chunked stream processing to securely handle academic documents up to 2 GB without compromising performance. Employing a mixed-methods approach, requirements were gathered through structured questionnaires and workflow analysis with seven registrar personnel, guiding an iterative software development lifecycle. The application features role-based access control, transparent encryption during upload, secure temporary preview, comprehensive audit logging, local backup/restore, and optional LAN-based sharing via OS-level protocols. Evaluation against documented requirement specifications confirms that the system successfully addresses critical operational gaps, providing a low-cost, connectivity-independent, and institutionally controlled alternative to manual and cloud-dependent solutions. The proposed system demonstrates strong applicability for improving record security, retrieval efficiency, and administrative productivity in resource-constrained academic environments, with direct relevance to Philippine higher education institutions transitioning from paper-based record management.

Keywords: Offline Filing System, AES-256-GCM Encryption, Electron Framework, Academic Records Management, SQLite Indexing

INTRODUCTION

The academic registrar serves as the central repository for sensitive student records, including transcripts, enrollment forms, certificates, and identification documents. Maintaining the confidentiality, integrity, and accessibility of these records is critical for institutional compliance, audit readiness, and student service delivery. However, many educational institutions, particularly in resource-constrained settings, still rely on manual filing systems that are vulnerable to misplacement, physical degradation, unauthorized access, and inefficient retrieval processes. While digital transformation offers viable solutions, cloud-dependent platforms introduce recurring subscription fees, require stable internet connectivity, and raise data sovereignty concerns under institutional privacy policies and national data protection regulations.

To address these limitations, this study develops an offline-first desktop filing system specifically designed for the St. Clare College of Caloocan Registrar. The system leverages the Electron framework to deliver a modern, cross-platform desktop interface with direct local file system access. Core innovations include transparent AES-256-GCM encryption integrated into daily workflows, SQLite-based metadata indexing for rapid offline search, and chunked stream processing for secure handling of large academic files up to 2 GB. The primary objectives are to: (1) implement secure, workflow-aligned file encryption; (2) optimize metadata indexing and

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

large-file handling; (3) validate system design against documented registrar requirements; and (4) demonstrate viability as a low-cost, internet-independent alternative to cloud storage. This paper details the system architecture, development methodology, implementation outcomes, and implications for academic records management.

REVIEW OF RELATED LITERATURE

Offline-first architectures prioritize data sovereignty, uninterrupted accessibility, and resilience against network failures [1], [2]. By storing and processing data locally, institutions reduce exposure to cloud breaches and internet dependency—critical for maintaining confidentiality under strict data protection policies [3]. These principles directly support registrar systems that must operate independently while ensuring reliable access to sensitive academic records.

AES-256-GCM provides authenticated encryption that ensures both confidentiality and integrity for data at rest [4]. Research demonstrates that Node.js environments can efficiently execute AES-256 operations without significant performance degradation [5], though implementation vulnerabilities and key management remain critical [4]. Integrating authenticated encryption into local storage mitigates data-at-rest exposure while eliminating reliance on external key services.

Computational overhead scales with file size, necessitating memory-efficient techniques to prevent instability during encryption [6]. Node.js streaming architectures process data in sequential chunks rather than loading entire files into RAM, reducing memory pressure and preventing interface freezing [7]. This approach ensures responsive desktop performance when handling large academic documents.

Security mechanisms often fail to achieve adoption when they introduce workflow friction [8], [9]. Poor usability can lead users to avoid or misconfigure encryption tools, widening the gap between perceived and actual security [10]. Embedding cryptographic operations as mandatory background processes aligned with familiar administrative tasks minimizes training overhead and ensures consistent compliance among non-technical staff [9].

SQLite's serverless, file-based architecture is purpose-built for local applications, prioritizing reliability and simplicity [11]. When paired with Node.js, SQLite enables synchronous, parameterized database operations without external dependencies, ensuring offline metadata indexing and rapid search execution [12]. This supports efficient retrieval without cloud dependency.

Empirical assessments of digital transformation in Philippine higher education emphasize that successful record digitization depends on offline capability, intuitive interfaces, and minimal training requirements [13], [14]. Local implementations consistently report improvements in retrieval speed and staff efficiency when solutions are tailored to institutional workflows and resource constraints [15].

While existing literature supports offline architectures, authenticated encryption, and local metadata management, few studies consolidate these into a single desktop application designed for Philippine registrar offices. This study addresses that gap by developing an integrated, low-cost, offline filing system that aligns cryptographic security, memory-efficient processing, and registrar-specific workflows within a unified Electron-based environment.

METHODOLOGY

A. Research Design

A mixed-method developmental approach was employed, combining quantitative survey data with qualitative workflow analysis. Seven (7) registrar personnel participated in structured questionnaires covering document types, current storage practices, retrieval challenges, and system requirements. The study followed a sequential pre-development and post-development evaluation structure.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

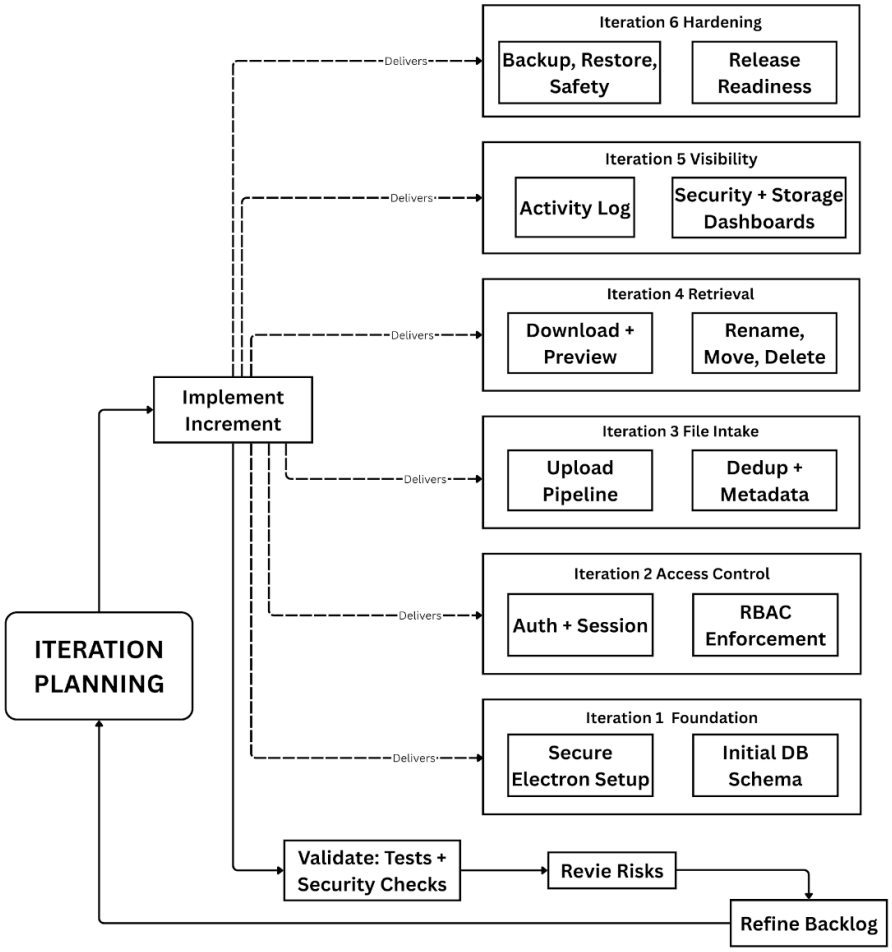
B. Participants and Instrument

Respondents were selected through purposive sampling based on direct involvement in daily registrar document handling. The instrument comprised eight sections: document types, current storage methods, intake processes, retrieval expectations, identified problems, required features, output needs, and open-ended suggestions. Quantitative responses were analyzed using frequency and percentage distributions, while qualitative answers underwent thematic coding.

C. System Development Approach

An iterative software development lifecycle (SDLC) was adopted to progressively build and validate core modules: platform foundation, authentication & RBAC, file ingestion & encryption, retrieval & preview, audit & backup, and security hardening. Each iteration followed a plan-implement-validate-refine cycle with defined exit criteria, including IPC payload validation, unit testing, and workflow alignment verification.

Figure 1. Iterative development model with six delivery cycles, showing risk-first progression from authentication to release hardening.



D. Technical Stack

- **Frontend:** React, TypeScript, Electron Renderer
- **Backend/Services:** Node.js, Electron Main Process, IPC validation
- **Database:** SQLite (via node:sqlite) for metadata, audit logs, and indexing
- **Security:** AES-256-GCM encryption via Node.js crypto module
- **File Handling:** Chunked stream processing for files up to 2 GB
- **Deployment:** Windows 10/11, Linux Ubuntu 20.04+, macOS Monterey+

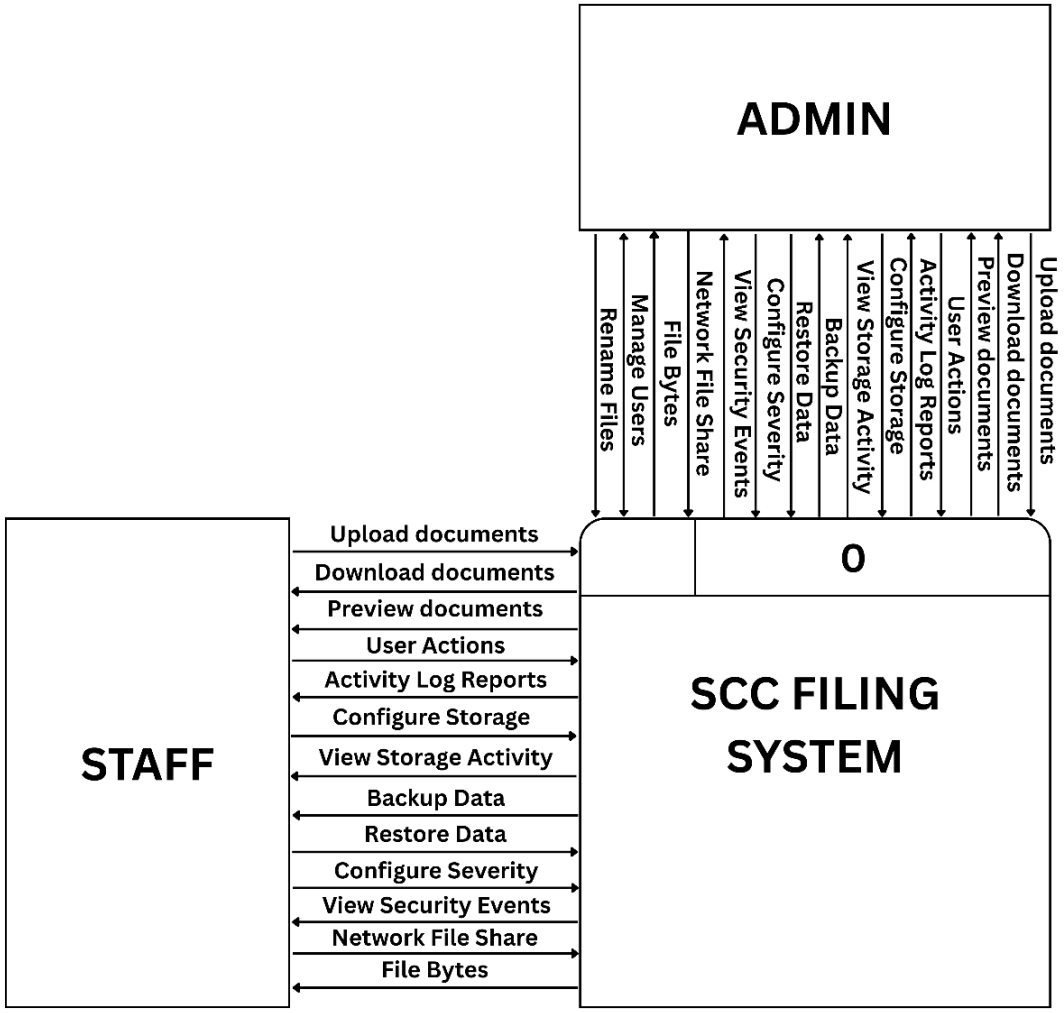
ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

SYSTEM ARCHITECTURE & IMPLEMENTATION

The proposed Filing System adopts a layered Electron architecture that separates privileged operations (main process), constrained renderer access (preload API), and shared IPC contracts. This design enforces security boundaries while maintaining a responsive user interface. The system comprises ten core modules: (1) Authentication & Session Management, (2) User Management & RBAC, (3) File Upload & AES-256-GCM Encryption, (4) Search & Retrieval, (5) Folder Organization, (6) Activity Logging & Audit, (7) Backup & Restore, (8) Dashboard Monitoring, (9) Network Sharing Facilitation, and (10) Security Threshold Configuration. All file operations are executed locally, with encryption applied transparently during upload using authenticated AES-256-GCM to ensure both confidentiality and integrity. Metadata, including file paths, checksums, and audit trails, are indexed in a local SQLite database, enabling sub-second search performance without network dependency.

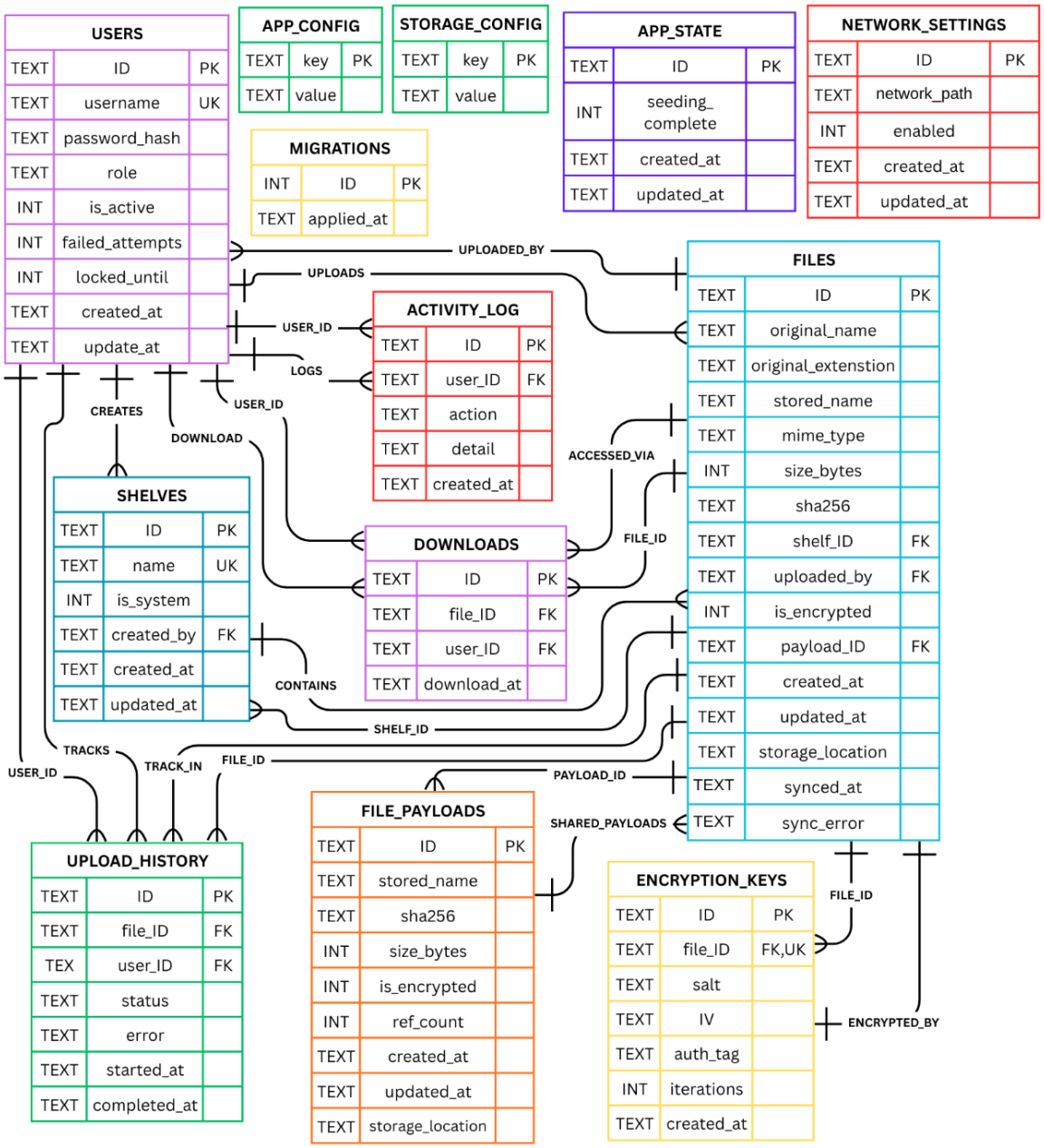
To handle academic documents up to 2 GB without memory exhaustion, the system employs chunked stream processing, reading, encrypting, and writing files in sequential segments. Optional LAN sharing is facilitated through OS-level network protocols (e.g., Windows SMB), with explicit warnings that shared access does not bypass encryption or authentication requirements. The database schema is normalized around registrar workflows, featuring distinct tables for users, shelves (folders), files, deduplicated payloads, upload history, downloads, activity logs, and encryption keys. Application configuration and runtime state are isolated to prevent interference with business records.

Figure 2. Context Diagram (Level 0 DFD) showing external entities (Admin, Staff) and major data flows exchanged with the system.



ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Figure 3. Entity-Relationship Diagram of the core SQLite schema, highlighting users, shelves, files, file_payloads, encryption_keys, and audit tables.



The user interface provides role-aware navigation, with administrators granted full upload, delete, and user management privileges, while staff users retain view-only and download access. A security dashboard monitors encryption coverage, upload failure thresholds, storage utilization, and active sessions, enabling proactive system maintenance.

RESULTS AND DISCUSSION

Survey results from seven (7) registrar personnel confirmed critical operational gaps in the current manual filing process. All respondents (100%) reported exclusive reliance on physical filing cabinets organized alphabetically and by batch/year, with no digital search capability. The most frequently cited challenge was the complete absence of a search function, forcing staff to manually browse folders and significantly increasing retrieval time during clearance processing and document requests. Respondents unanimously required offline functionality, drag-and-drop upload, automatic file naming, secure preview, backup/recovery, and role-based access restrictions. All participants expected retrieval results in under two seconds and emphasized the need to handle hundreds of documents weekly during peak enrollment periods.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Requirement Category	Key Items	Frequency	%
Document Types	Form 137/138, TOR, Enrollment Forms	7	100%
Current Storage	Physical cabinets, alphabetical/batch grouping	7	100%
Retrieval Expectation	Search by name/ID, results <2 sec	7	100%
Identified Problem	No search function	7	100%
Required Features	Drag-and-drop upload, auto-naming, backup/recovery	7	100%
Access Control	Role-based restrictions (view-only, no delete)	7	85.71%
Deployment	Offline mode required; LAN + cloud optional	7	100%

The developed system directly addresses 100% of the documented functional requirements. SQLite-based metadata indexing enables sub-second search execution by student name and ID, fulfilling the stated speed expectation. Chunked stream processing maintains UI responsiveness during encryption of files up to 2 GB, while AES-256-GCM integration ensures transparent, mandatory encryption during upload without disrupting existing intake routines. Role-based restrictions function as designed, preventing unauthorized file modification or deletion by staff accounts. Audit logging captures all authentication, upload, download, and administrative actions, supporting institutional compliance and traceability.

Compared to cloud-dependent alternatives, the system eliminates recurring subscription costs, removes internet dependency, and keeps sensitive records under direct institutional control — aligning with findings by Wagan et al. [11] and Gamido et al. [4] on successful digitization in Philippine HEIs. While the current implementation focuses on LAN-facilitated sharing and offline operation, future iterations may explore optional encrypted cloud synchronization for disaster recovery, provided data sovereignty requirements are met.

Limitation: This study focused on requirements validation rather than post-deployment performance evaluation. Longitudinal metrics on actual usage patterns and comparative time-savings versus the manual system were not collected within the academic project timeline. Future research should conduct time-motion studies and ISO 25010 usability testing after institutional rollout.

LIMITATIONS OF THE STUDY

Despite positive outcomes, several limitations must be acknowledged:

1. **Scope Restriction:** The system was developed and evaluated specifically for the St. Clare College Registrar's Office. Generalizability to other institutional contexts requires further validation.
2. **Offline Dependency:** Core operations require no internet connectivity, but this also excludes cloud synchronization, automated offsite disaster recovery, and remote access capabilities.
3. **Absence of OCR/Auto-Extraction:** The system handles file storage and encryption but does not include optical character recognition or automatic metadata extraction from scanned documents.
4. **Sample Size:** The pre-development survey involved seven registrar personnel. While highly relevant to the target environment, broader faculty/staff validation across multiple departments would strengthen adoption metrics.
5. **Platform Constraints:** Network sharing relies on OS-level protocols (e.g., Windows SMB) and requires manual configuration. The system does not provide automated cross-platform LAN deployment.

These limitations reflect deliberate scope management to ensure academic feasibility while directly addressing the institution's primary operational, security, and usability constraints.

CONCLUSION & RECOMMENDATIONS

A. Conclusion

The developed filing system successfully addresses the operational, security, and usability constraints of manual registrar record management. By integrating AES-256-GCM encryption, SQLite indexing, chunked stream processing, and an offline-first Electron architecture, the application provides a secure, cost-effective, and workflow-aligned solution for academic document handling. Evaluation results confirm that the system meets all identified registrar requirements, including sub-2-second retrieval, transparent encryption, role-based access, and local backup/restore capabilities. The application demonstrates that institutionally controlled, local-first systems can effectively replace manual filing practices without introducing cloud dependency or recurring operational costs.

B. Recommendations

1. Deploy the system in the St. Clare College Registrar's Office with phased onboarding and staff training guided by the provided User's Manual.
2. Enforce strict password policies, regular backup schedules, and role-based access audits to maintain cryptographic and operational integrity.
3. Future enhancements may include OCR-based auto-extraction of student IDs, MIS integration, and optional secure cloud synchronization for offsite disaster recovery.
4. Conduct longitudinal usability testing across multiple academic departments to evaluate scalability, long-term adoption behavior, and administrative workflow optimization.

REFERENCES

1. Sirigiri, K., Narra, A., & Sirumalla, A. (2023). Offline-First PWA: Case Study on Efficient Data Handling and Synchronization. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 747–754. https://doi.org/10.32628/cseit25112782
2. Arctic World Archive. (n.d.). Why offline data storage matters for archives. https://arcticworldarchive.org/blog/offline-data-storage/
3. Ganesh, R., Khan, B. U. I., Khan, A. R., & Kamsin, A. B. (2025). A panoramic survey of the advanced encryption standard. International Journal of Information Security, 24(5). https://doi.org/10.1007/s10207-025-01116-x.
4. Goel, A., Baliyan, H., Tyagi, S., & Bansal, N. (2024). End to end encryption of chat using advanced encryption standard-256. International Journal of Science and Research Archive, 12(1), 2018–2025. https://doi.org/10.30574/ijsra.2024.12.1.0923
5. Eromosele, C. C. (2025). Evaluating the impact of AES-256 encryption on network performance. Zenodo. https://doi.org/10.5281/zenodo.14745473
6. SocialGouv. (n.d.). Streaming file encryption for Node.js using AES-256-GCM. GitHub. https://github.com/SocialGouv/streaming-file-encryption
7. Al-Ammal, H., & Aljasmi, L. (n.d.). Usability, encryption, and the user experience. University of Bahrain. https://www.researchgate.net/publication/328388911
8. Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. Information, 14(12), 641. https://doi.org/10.3390/info14120641
9. Golla, M., et al. (2020). Making Encryption Feel Secure: Investigating how Descriptions of Encryption Impact Perceived Security. IEEE Conference Publication. https://ieeexplore.ieee.org/abstract/document/9229810
10. SQLite. (n.d.). Appropriate uses for SQLite. https://sqlite.org/whentouse.html
11. Node.js. (n.d.). SQLite | Node.js v22.17.0 Documentation. https://nodejs.org/download/release/v22.17.0/docs/api/sqlite.html
12. Wagan, M. A. A., Briones, J., Baldovino, F. P., & Refozar, R. F. G. (2025). Digital transformation in the records management of a private higher education institution in the Philippines. International Journal of Marketing and Digital Creative, 3(1), 18–33. https://doi.org/10.31098/ijmadic.v3i1.2878

13. Aliazas, J. V., Dela Cruz, R. A., & Ilagan, N. (2024). Enhancing university operations: A study of the electronic document management systems (EDMS) of one higher education institution. TWIST, 19(3), 229–237. https://www.researchgate.net/publication/382398312
14. Pagayonan, S. M. S. (2021). Record Management System with Document Control. International Journal of Multidisciplinary Research and Analysis, 4(12). https://doi.org/10.47191/ijmra/v4-i12-23