



A Forensic-Centric Security Framework for Financial Database Systems.

Submitted By,

Anisha Karottupalathumkal Sreedhar

Supervisor: Suresh Suresh Shanmugasundaram

Introduction

- For the banking and financial services industry, core database systems are the backbone of its business, supporting all essential operations, such as real-time transactions, client portfolio management, and regulatory reporting adherence [1]. The paradoxical institutional risk is that the systems most critical to the business are also the most appealing to the bad guys looking for financial gain, competitive intelligence, or to disrupt the business [7]
- In this case, databases are the ones that are essential to the organisation, and at the same time hold the most sensitive financial data, including account information, transaction histories, and personally identifiable information (PII). The threat landscape facing financial databases is especially dire, with threats including advanced persistent threats (APTs) that steal data over a prolonged period without a traditional detection method, ransomware targeting important financial data, and insider threats from employees with privileged access, as well as advanced external attack vectors like SQL injection
- The security of databases within financial institutions has followed a general pattern of the evolution of technology: starting with basic access control mechanisms to limit access to teller systems and database administrators, moving on to strong encryption of data at rest (DAR) required by the Payment Card Industry Data Security Standard (PCI DSS), and finally to more sophisticated real-time monitoring architectures that aid in fraud detection and anomaly identification [2], [3].

Problem Statement

- Current database security architectures are built to be reactive, focusing resources on containment after a breach and on defending the perimeter, but not on the proactive, ongoing forensic evidence preservation necessary to an effective post-breach investigation — an approach that can result in long investigations during time-sensitive financial incidents [7].
- Forensic processes for database breaches in financial institutions are not standardised or consistent across the industry, and often do not comply with the high evidentiary standards expected in financial litigation and regulatory examinations – with direct legal and compliance implications for institutions subject to GDPR, PCI DSS [9].
- Third and most importantly for the current study, there is no single framework available that combines proactive security measures with digital forensics readiness specifically tailored to meet the compliance, legal admissibility and operational requirements of the banking sector [7]. This three-part gap leaves financial institutions institutionally vulnerable to significant operational, reputational and financial harm, unable to effectively gather and retain admissible digital evidence.

Aim & Objective

The goal of this research is to create and validate a complete Digital Forensics Readiness Framework (DFRF) for financial database systems of banking sector. The four objectives that will be used to achieve this aim are:

1. To investigate current database security architectures, database forensics readiness models, and financial incident investigation procedures, and determine key gaps and needs of a forensic ready financial database system.
2. To create a Digital Forensics Readiness Framework (DFRF) for financial databases that integrates best practices from both database security and digital forensics, includes essential banking-specific elements such as risk assessment, and encryption of data-at-rest and data-in-transit.
3. To ensure that the proposed DFRF will be in line with international standards and frameworks, primarily ISO/IEC 27037:2012.
4. To evaluate correctness, forensic utility and ISO/IEC 27037:2012 contribution of a layer of AES-256 encryption implemented using Python and SQLite, as a validated component of the DFRF and using the principles of transparent data encryption (TDE) and a two-tier key management architecture to provide layered data-at-rest protection.

Literature Review

Key Themes

Key Findings & Gaps Identified

Database Security Frameworks

Reactive models, forensics as afterthought [1,2]. Encryption hinders acquisition if keys undocumented [9]. Logs lack integrity, inadmissible [1]. Advanced controls fail forensic readiness [3,5].

Digital Forensics Readiness Models

Proactive forensics improves admissibility [3,4]. Generic DFR models ignore banking databases (structure, volume, regulations) [1,6,7]. Gap: No banking-specific DFR model.

Incident Investigation Processes

Cannot distinguish insider threats [5,8]. Banks lack procedures, trained staff, toolchains [4]. Result: broken chain of custody [4,5].

Regulatory Standards (ISO/IEC 27037, PCI DSS v4.0)

ISO 27037 mandates chain of custody but no database guidance [3]. PCI DSS v4.0 requires logs, not systematic preservation [10]. No guidance for live transactions, encrypted storage [3,4]. Gap: Standards not operationalised for banking databases.

Cross-Thematic Synthesis

Three gaps: (1) Reactive architectures = no admissible evidence; (2) Generic DFR models lack banking specificity; (3) Standards lack integration for financial databases [1,2,4,5]. No framework combines proactive security, forensic logging, live acquisition, and compliance [2].

Methodology

There are three main research philosophies that has considered for this study: positivism, interpretivism and pragmatism.

- The positivist belief that knowledge can only be gained from observable and measurable phenomena, and the emphasis on quantitative research and value-free, objective research
- Interpretivism emphasizes the subjective meanings that actors give to the social phenomena, and is similarly out of place with a study focusing on the construction of artefacts and the implementation of techniques, but not on human experiences .
- Pragmatism addresses this dichotomy by assessing research methods instrumentally, that is, based on their suitability for the research problem, rather than on an a priori ontological commitment, thus allowing for the use of a variety of research methods

This study is based on a pragmatist philosophy paradigm which is a paradigm that argues that the value of knowledge is not only determined by the logical consistency of it, but also by the usefulness of knowledge in solving problems in the real world

In the pragmatist paradigm, this study uses a constructivist ontology, which assumes that the DFRF is a constructed artefact, influenced by the existing frameworks, standards and design decisions, rather than the empirical reality

Research Approach and Strategy

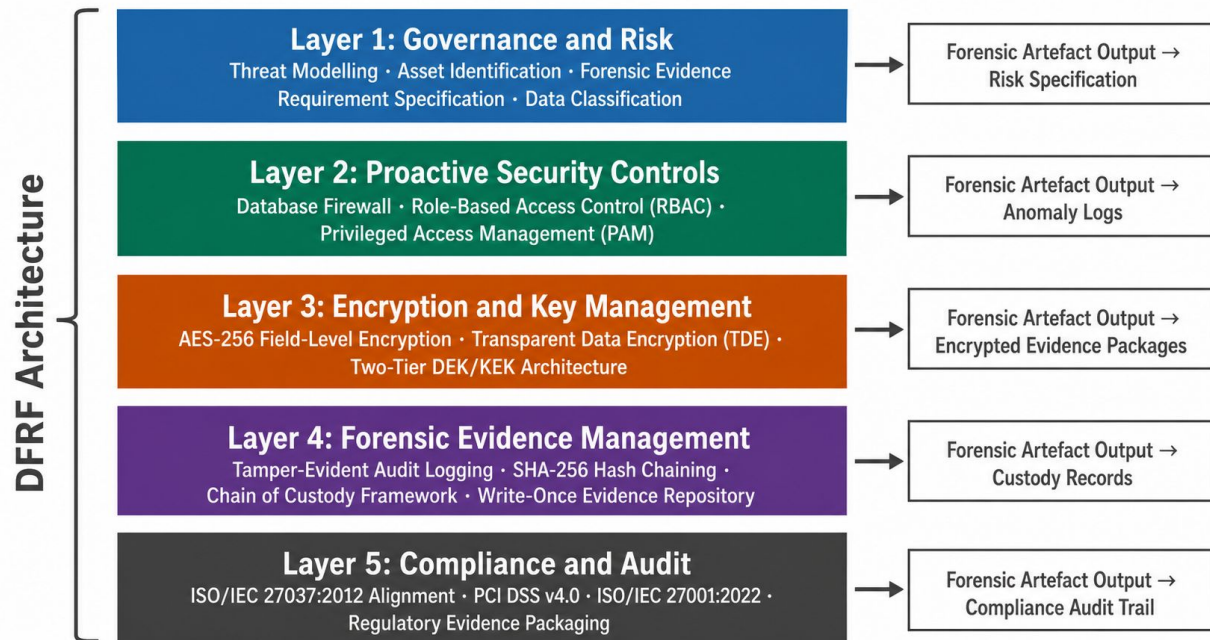
The overall research approach used in this study is Design Science Research (DSR)

- Widely used research approach in the field of Information Systems (IS) and Cybersecurity research and views the creation of knowledge as the design, construction, and systematic evaluation of an intentional artefact that is designed to solve a problem in an organization or a technical system [8].
- DSR is the most appropriate method for this study since the main product of DSR — the DFRF — is exactly the sort of artefact that DSR is meant to build and test

This study follows Peffers DSR methodology model, which goes through six phases: problem identification and motivation, objective definition, design and development, demonstration, evaluation, and communication – each of which is represented by a chapter in this dissertation.

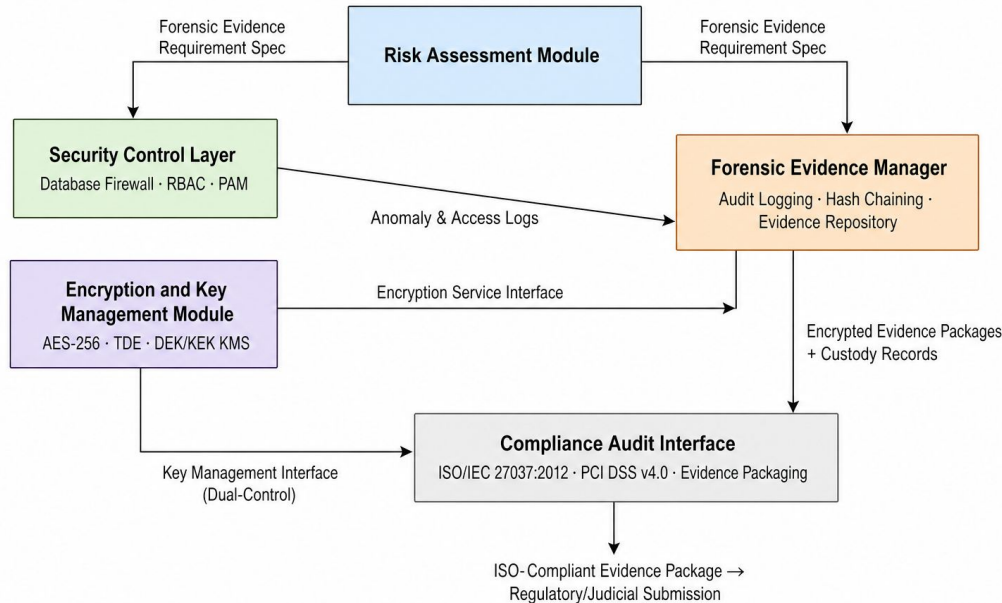
No primary data from humans have been collected for this study. The analytical inputs used have been collected from secondary sources (peer-reviewed journal articles, international standards, technical documentation and regulatory frameworks)

Design Process



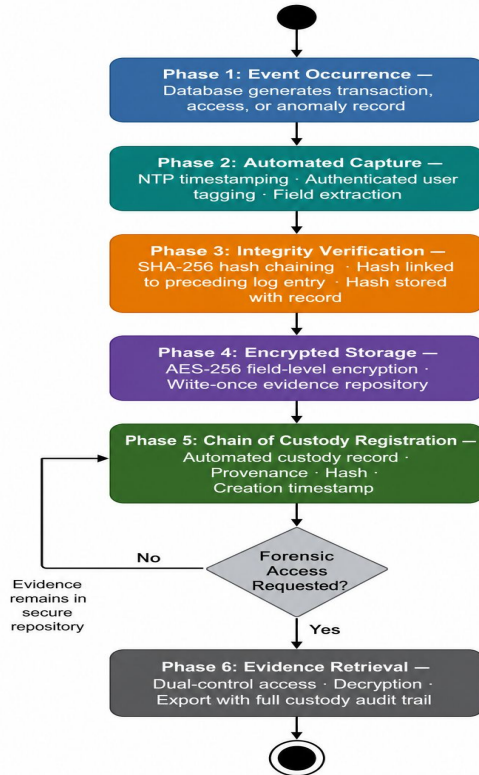
The DFRF aims to be a five-layer framework with each layer covering a separate aspect of forensic readiness in the banking database environment: (1) Governance and Risk, (2) Proactive Security Controls, (3) Encryption and Key Management, (4) Forensic Evidence Management, and (5) Compliance and Audit

Component Diagram



The DFRF component diagram shows five main components (Risk Assessment Module, Security Control Layer, Encryption and Key Management Module, Forensic Evidence Manager and Compliance Audit Interface) connected via specific interfaces, which control the movement of forensic evidence artefacts between components.

Activity Diagram: Forensic Evidence Lifecycle



The forensic evidence lifecycle activity diagram represents a series of activities in a sequential manner beginning with the event in the database and ending with the evidence package being submitted for forensic analysis, a process that includes six phases:

Event Occurrence, Automated Capture, Integrity Verification, Encrypted Storage, Chain of Custody Registration, and Evidence Retrieval.

Implementation

- **Synthetic Database Environment** : The implementation consists of a SQLite relational database that mimics the transactional nature of a retail banking system and consists of four main tables: accounts, transactions, audit_log and key_store.
- **AES-256 Field-Level Encryption** : The AES-256 field-level encryption layer is achieved by using the cryptography library- hazmat
- **Two-Tier Key Management Architecture** : In the two-tier key management architecture that is used in the DFRF, there are two different types of keys: Data Encryption Keys (DEKs) and Key Encryption Keys (KEKs)
- **Tamper-Evident Audit Logging**: Using hash chaining with the SHA-256 algorithm, it generates an audit log of all the database operations that is sequentially linked and immutable, with each log operation containing the hash of the previous operation

```
import sqlite3, hashlib, os, secrets
from datetime import datetime

conn = sqlite3.connect('banking_dfrf.db')
cursor = conn.cursor()

cursor.execute('''
    CREATE TABLE IF NOT EXISTS transactions (
        tx_id          INTEGER PRIMARY KEY AUTOINCREMENT,
        account_from   TEXT    NOT NULL,
        account_to      TEXT    NOT NULL,
        amount_enc      BLOB    NOT NULL,
        created_at      TEXT    NOT NULL,
        modified_by     TEXT    NOT NULL,
        record_hash     TEXT    NOT NULL
    )
''')
```

Evaluation

Test ID	Component Tested	Test Objective	Input Condition	Expected Output	Pass/Fail
TC-01	AES-256 encryption	Verify ciphertext produced from plaintext field	Account number string (16 chars)	Base64-encoded BLOB; plaintext not recoverable without DEK	Pass
TC-02	AES-256 decryption	Verify correct plaintext recovered with valid DEK	Encrypted BLOB + correct DEK	Original plaintext string returned	Pass
TC-03	AES-256 tamper detection	Verify InvalidTag raised on corrupted ciphertext	Encrypted BLOB with one byte modified	cryptography.exceptions.InvalidTag exception raised	Pass
TC-04	DEK/KEK wrapping	Verify DEK encrypted under KEK (envelope encryption)	32-byte DEK + derived KEK	Wrapped DEK BLOB stored; raw DEK not persisted in plaintext	Pass
TC-05	DEK/KEK unwrapping	Verify DEK correctly recovered under forensic access	Wrapped DEK BLOB + correct KEK	Original 32-byte DEK returned	Pass
TC-06	DEK/KEK wrong key	Verify recovery fails with incorrect KEK	Wrapped DEK BLOB + incorrect KEK	cryptography.exceptions.InvalidTag raised	Pass
TC-07	Hash chain integrity	Verify each log entry hash incorporates preceding hash	Sequential log entries (n=10)	Each entry's prev_hash matches preceding entry's log_hash	Pass

Conclusion

- The goal of the dissertation was to develop and validate a Digital Forensics Readiness Framework (DFRF) for banking institutions, which combines proactive security measures with readiness for digital evidence collection, preservation, and analysis to ensure the acquisition of admissible digital evidence following a security incident.
- This objective was completely met: Objective 1 identified 4 structural gaps in existing models, Objective 2 provided a 5-layer DFRF architecture, incorporating STRIDE risk assessment, RBAC/PAM, and AES-256 encryption, and Objective 4 generated a working prototype of AES-256 encryption for Python and SQLite, though there were minor documentation issues.
- The framework offers a new, standards-based and banking-specific solution that connects proactive security and forensic readiness.

References

1. A. Albugmi, "Digital Forensics Readiness Framework (DFRF) to secure database systems," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 2, pp. 13732–13740, Apr. 2024.
2. A. Faizal and A. Luthfi, "Comparison study of NIST SP 800-86 and ISO/IEC 27037 standards as a framework for digital forensic evidence analysis," *J. Inf. Syst. Inform.*, vol. 6, no. 2, pp. 701–718, 2024.
3. S. Mukamurenzi, T. P. Abayomi-Zannu, and N. Ntlatlapa, "Towards digital forensic readiness: a framework for financial service providers," *East Afr. J. Inf. Technol.*, vol. 7, no. 1, pp. 92–107, Apr. 2024.
4. V. R. Kebande, H. S. Venter, and I. Ray, "An extended digital forensic readiness and maturity model," *Forensic Sci. Int.: Digit. Invest.*, vol. 40, article 301330, Mar. 2022.
5. I. Kanani, "Securing data at rest: evaluating encryption strategies for databases and file systems," *Int. J. Multidiscip. Res.*, vol. 3, no. 2, pp. 1–10, 2021.
6. K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manage. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007.
7. ISO, *ISO/IEC 27037:2012 — Information Technology: Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva: ISO, 2012.
8. ISO, *ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems: Requirements*. Geneva: ISO, 2022.
9. PCI Security Standards Council, *PCI DSS v4.0: Payment Card Industry Data Security Standard*. Wakefield, MA: PCI SSC, 2022. [Online]. Available: <https://www.pcisecuritystandards.org>