CHƯƠNG 4: THỰC NGHIỆM VÀ KẾT QUẢ

4.1. Giới thiệu

- Mục tiêu thực nghiệm
- Phạm vi đánh giá

4.2. Trình bày dữ liệu (Presentation of Data)

4.2.1. Môi trường triển khai

4.2.2. Dữ liệu thử nghiệm

4.2.3. Ma trận kịch bản kiểm thử (Test Matrix)

4.3. Phân tích kết quả (Analysis of Results)

4.3.1. Đánh giá Layer 1: Xác thực (Keycloak)

4.3.2. Đánh giá Layer 2: Ủy quyền (OPA/ABAC)

4.3.3. Đánh giá Layer 3: WAF

4.3.4. Đánh giá Layer 4: Toàn vẹn log (Anchor Hash)

4.4. Diễn giải kết quả (Interpretation of Results)

4.4.1. Tỷ lệ tuân thủ tổng thể

4.4.2. Phân tích các trường hợp fail

4.5. So sánh với tài liệu (Comparison with Literature)

4.6. Ý nghĩa kết quả (Implications)

4.7. Tóm tắt chương

NỘI DUNG CHI TIẾT TỪNG SECTION

4.1. Giới thiệu (~0.5 trang)

- Mục tiêu: Đánh giá khả năng phát hiện vi phạm tuân thủ của hệ thống
- Phạm vi: Focus vào compliance monitoring cho SME y tế VN
- Phương pháp: Scenario-based testing

4.2. Trình bày dữ liệu (~2 trang)

4.2.1. Môi trường triển khai

Thành phần	Cấu hình
Server	Windows Server / Docker Compose
Database	MariaDB 10.11
IAM	Keycloak 23.0.0
Policy Engine	OPA latest
Gateway	NGINX OpenResty

4.2.2. Dữ liệu thử nghiệm

Metric	Số lượng
Số users	15-20 tài khoản
Số roles	11 vai trò
Số bệnh nhân	50-100 hồ sơ
Số logs thu thập	X,XXX bản ghi
Thời gian thu thập	1 tuần

4.2.3. Ma trận kịch bản (21 test cases)

#	Role	Action	Context	Expected	Actual
1	Doctor	View patient	In care team	ALLOW	?
2	Doctor	View patient	NOT in care team	DENY	?
3	Nurse	Update vitals	In care team	ALLOW	?
...	...	...	...	...	...
21	Admin	Delete logs	-	DENY	?

4.3. Phân tích kết quả (~3 trang)

4.3.1. Layer 1: Xác thực (Keycloak)

- Số lần login thành công: X
- Số lần login thất bại: Y
- Brute-force detected: Z lần

4.3.2. Layer 2: Ủy quyền (OPA/ABAC)

- Số request ALLOW: X
- Số request DENY: Y
- Bảng chi tiết theo role
- Bảng chi tiết theo purpose

4.3.3. Layer 3: WAF (nếu có)

- SQL Injection blocked: X
- XSS blocked: Y

4.3.4. Layer 4: Toàn vẹn log (Anchor Hash)

- Số lần chạy anchor hash: X
- Phát hiện anomaly: Y/N
- Mô tả simulation: xóa thử 10 logs → hệ thống phát hiện

4.4. Diễn giải kết quả (~1.5 trang)

4.4.1. Tỷ lệ tuân thủ

Accuracy = (Passed / Total) × 100%

= (18 / 21) × 100%

= 85.71%

4.4.2. Phân tích failures

Case #	Mô tả	Nguyên nhân fail	Đề xuất cải thiện
5	Doctor Oncology	Attribute mapping chưa đầy đủ	Bổ sung rules
...	...	...	...

4.5. So sánh với Literature (~0.5 trang)

- So với yêu cầu NIST SP 800-92: Đạt/Không đạt
- So với yêu cầu TT 46/2018: Đạt/Không đạt
- So với các SIEM thương mại: Chi phí, độ phức tạp

4.6. Ý nghĩa kết quả (~0.5 trang)

- Hệ thống phù hợp cho SME với độ chính xác 85%+
- Chi phí triển khai: 0đ (open-source)
- Thời gian triển khai: 2-3 ngày

4.7. Tóm tắt chương (~0.5 trang)

- Tóm tắt kết quả chính
- Kết nối với Chapter 5 (Discussion)

BẢNG/BIỂU ĐỒ NÊN CÓ

1. **Bảng 4.1:** Môi trường triển khai
2. **Bảng 4.2:** Ma trận 21 test scenarios
3. **Bảng 4.3:** Kết quả theo Layer

4. **Biểu đồ 4.1:** Tỷ lệ ALLOW/DENY theo role
5. **Biểu đồ 4.2:** Vi phạm theo thời gian
6. **Bảng 4.4:** Phân tích failures