# 3.1 STRIDE Threat Analysis Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Category | Risk Level | Mitigation | Implementation |
| Spoofing | Medium | Password Hashing | Werkzeug check\_password\_hash |
| Tampering | Low | AES-GCM Auth | Authentication tags |
| Repudiation | Low | Cryptographic Binding | Master Key derivation |
| Information Disclosure | Low | Client-side Encryption | Web Crypto API |
| Denial of Service | High | Operational Controls | Backup/Redundancy |
| Elevation of Privilege | Low | Key Separation | Hierarchical keys |

# 3.2 Attack Vector Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack Vector | Probability | Impact | Risk Score | Mitigation |
| Server Compromise | Medium | Low | Medium | Zero-knowledge design |
| Password Brute Force | High | High | High | PBKDF2 + High iterations |
| Man-in-the-Middle | Low | Medium | Low | HTTPS/TLS |
| Client Malware | Medium | High | High | Out of scope |
| Code Injection | Low | High | Medium | CSP headers |

# 3.3 Cryptographic Primitive Comparison

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Algorithm | Key Size | Performance | Security Level | Browser Support |
| PBKDF2 | N/A | Fast | Good | Native |
| Argon2 | N/A | Medium | Excellent | Library Required |
| AES-GCM | 256-bit | Very Fast | Excellent | Native |
| ChaCha20-Poly1305 | 256-bit | Fast | Excellent | Limited |

# 4. PERFORMANCE ANALYSIS CHARTS

## 4.1 PBKDF2 Performance vs Security Table

|  |  |  |  |
| --- | --- | --- | --- |
| Iterations | Derivation Time (ms) | Attacker Cost Multiplier | User Experience |
| 10,000 | 28 | 1x | Excellent |
| 50,000 | 140 | 5x | Good |
| 100,000 | 275 | 10x | Acceptable |
| 500,000 | 1,375 | 50x | Poor |
| 1,000,000 | 2,750 | 100x | Unacceptable |

## 4.2 File Size vs Encryption Time

|  |  |  |  |
| --- | --- | --- | --- |
| File Size | Encryption Time | Decryption Time | Upload Time |
| 1 MB | 15ms | 12ms | 2.3s |
| 10 MB | 125ms | 108ms | 8.7s |
| 100 MB | 1.2s | 1.1s | 45s |
| 1 GB | 12.5s | 11.2s | 7.5min |

# 5. TESTING AND VALIDATION DIAGRAMS

## 5.1 Test Coverage Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Unit Tests | Integration Tests | Security Tests | Status |
| Key Derivation | ✓ | ✓ | ✓ | Pass |
| File Encryption | ✓ | ✓ | ✓ | Pass |
| API Endpoints | ✓ | ✓ | ✓ | Pass |
| Database Layer | ✓ | ✓ | ✓ | Pass |
| Frontend UI | - | ✓ | ✓ | Pass |

## 5.2 Security Test Results Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test ID | Test Name | Expected Result | Actual Result | Status |
| SVT-01 | Zero-Knowledge Verification | Server blind to plaintext | ✓ Confirmed | PASS |
| SVT-02 | Data Integrity | Tampering detected | ✓ Confirmed | PASS |
| SVT-03 | PBKDF2 Performance | Linear time increase | ✓ Confirmed | PASS |
| SVT-04 | Unique Salt Generation | Each user unique | ✓ Confirmed | PASS |
| SVT-05 | Key Unwrapping Errors | Wrong key fails | ✓ Confirmed | PASS |

# 6. COMPARATIVE ANALYSIS TABLES

## 6.1 CSE Solutions Comparison

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Solution | Architecture | Key Management | Browser Support | Usability |
| Your Prototype | Web-based | User-managed | Full | Good |
| Cryptomator | Desktop App | Password-based | N/A | Excellent |
| Boxcryptor | Hybrid | Cloud-assisted | Limited | Good |
| SpiderOak | Native Client | Server-managed | N/A | Fair |

## 6.2 Web Crypto API vs Alternatives

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | Web Crypto API | CryptoJS | Forge | Native App |
| Performance | Excellent | Good | Fair | Excellent |
| Security | High | Medium | Medium | High |
| Browser Support | Wide | Universal | Universal | N/A |
| Bundle Size | 0KB | 300KB | 500KB | N/A |
| Hardware Acceleration | Yes | No | No | Yes |

# 9. FUTURE WORK VISUALIZATION

## 9.1 Research Roadmap

|  |  |  |  |
| --- | --- | --- | --- |
| Phase | Timeline | Focus Area | Key Deliverables |
| Phase 1 | 3-6 months | Social Recovery | SSS implementation |
| Phase 2 | 6-12 months | Metadata Protection | PIR integration |
| Phase 3 | 12-18 months | Multi-user Sharing | PKI system |
| Phase 4 | 18-24 months | Post-Quantum | PQC algorithms |

# 10. IMPLEMENTATION COMPLEXITY MATRIX

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | Development Effort | Security Impact | User Benefit | Priority |
| Basic CSE | High | High | High | ✓ Complete |
| Social Recovery | Medium | Medium | High | Next |
| Metadata Protection | High | Medium | Medium | Future |
| File Sharing | Very High | High | High | Future |
| Mobile App | Medium | Low | High | Future |