

# Veri-Store Security Model

Mac Payton & Albert Huynh

February 16, 2026  
Version 0.1

## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Document Purpose . . . . .	4
1.2	System Overview . . . . .	4
<b>2</b>	<b>Scoping</b>	<b>4</b>
2.1	In Scope . . . . .	4
2.2	Out of Scope . . . . .	4
<b>3</b>	<b>Use Scenarios</b>	<b>4</b>
3.1	Primary Use Case . . . . .	4
3.2	Anti-Scenarios . . . . .	4
<b>4</b>	<b>Dependencies</b>	<b>4</b>
4.1	External Libraries . . . . .	4
4.2	System Dependencies . . . . .	4
<b>5</b>	<b>Implementation Assumptions</b>	<b>4</b>
<b>6</b>	<b>Trust Levels</b>	<b>5</b>
6.1	Administrator . . . . .	5
6.2	Authenticated Client . . . . .	5
6.3	Storage Server . . . . .	5
6.4	Untrusted Network . . . . .	5
<b>7</b>	<b>Entry Points</b>	<b>5</b>
7.1	Client API . . . . .	5
7.2	Inter-Server Communication . . . . .	5
7.3	Storage Subsystem . . . . .	5
<b>8</b>	<b>Protected Assets</b>	<b>7</b>
8.1	Data Blocks . . . . .	7
8.2	Erasure-Coded Fragments . . . . .	7
8.3	Homomorphic Fingerprints . . . . .	7
8.4	System Resources . . . . .	7

<b>9 Data Flow Diagram</b>	<b>7</b>
9.1 DFD Component Descriptions . . . . .	7
9.1.1 Client . . . . .	7
9.1.2 Encode Block . . . . .	7
9.1.3 Compute Fingerprint . . . . .	7
9.1.4 Distribute Fragments . . . . .	7
9.1.5 Network . . . . .	7
9.1.6 Fragment Storage . . . . .	7
9.1.7 Verify Fragments . . . . .	7
9.1.8 Reconstruct Block . . . . .	7
<b>10 Threat Analysis: STRIDE</b>	<b>7</b>
10.1 Spoofing . . . . .	7
10.1.1 S.1: Client Impersonation . . . . .	7
10.1.2 S.2: Server Impersonation . . . . .	7
10.1.3 S.3: Fingerprint Source Forgery . . . . .	7
10.2 Tampering . . . . .	7
10.2.1 T.1: Fragment Corruption in Storage . . . . .	7
10.2.2 T.2: Fragment Modification in Transit . . . . .	7
10.2.3 T.3: Fingerprint Tampering . . . . .	7
10.2.4 T.4: Erasure Code Parameter Manipulation . . . . .	7
10.3 Repudiation . . . . .	7
10.3.1 R.1: Anonymous Data Storage . . . . .	7
10.3.2 R.2: Fragment Deletion Without Logging . . . . .	7
10.3.3 R.3: Untrackable Verification Failures . . . . .	7
10.4 Information Disclosure . . . . .	7
10.4.1 I.1: Fragment Eavesdropping . . . . .	7
10.4.2 I.2: Storage Server Data Access . . . . .	7
10.4.3 I.3: Fingerprint Analysis . . . . .	7
10.4.4 I.4: Error Message Information Leakage . . . . .	7
10.5 Denial of Service . . . . .	7
10.5.1 D.1: Storage Exhaustion . . . . .	7
10.5.2 D.2: Fragment Unavailability . . . . .	7
10.5.3 D.3: Verification Flooding . . . . .	7
10.5.4 D.4: Network Bandwidth Exhaustion . . . . .	7
10.6 Elevation of Privilege . . . . .	7
10.6.1 E.1: Code Injection via Malformed Input . . . . .	7
10.6.2 E.2: Verification Bypass . . . . .	7
10.6.3 E.3: Cryptographic Parameter Override . . . . .	7
10.6.4 E.4: Server-to-Server Privilege Escalation . . . . .	7
<b>11 Threat Resolutions</b>	<b>7</b>
11.1 Spoofing Threat Resolutions . . . . .	7
11.1.1 S.1: Client Impersonation . . . . .	7
11.1.2 S.2: Server Impersonation . . . . .	8
11.1.3 S.3: Fingerprint Source Forgery . . . . .	8
11.2 Tampering Threat Resolutions . . . . .	8
11.2.1 T.1: Fragment Corruption in Storage . . . . .	8

11.2.2	T.2: Fragment Modification in Transit . . . . .	8
11.2.3	T.3: Fingerprint Tampering . . . . .	8
11.2.4	T.4: Erasure Code Parameter Manipulation . . . . .	9
11.3	Repudiation Threat Resolutions . . . . .	9
11.3.1	R.1: Anonymous Data Storage . . . . .	9
11.3.2	R.2: Fragment Deletion Without Logging . . . . .	9
11.3.3	R.3: Untrackable Verification Failures . . . . .	9
11.4	Information Disclosure Threat Resolutions . . . . .	9
11.4.1	I.1: Fragment Eavesdropping . . . . .	9
11.4.2	I.2: Storage Server Data Access . . . . .	10
11.4.3	I.3: Fingerprint Analysis . . . . .	10
11.4.4	I.4: Error Message Information Leakage . . . . .	10
11.5	Denial of Service Threat Resolutions . . . . .	10
11.5.1	D.1: Storage Exhaustion . . . . .	10
11.5.2	D.2: Fragment Unavailability . . . . .	10
11.5.3	D.3: Verification Flooding . . . . .	11
11.5.4	D.4: Network Bandwidth Exhaustion . . . . .	11
11.6	Elevation of Privilege Threat Resolutions . . . . .	11
11.6.1	E.1: Code Injection via Malformed Input . . . . .	11
11.6.2	E.2: Verification Bypass . . . . .	11
11.6.3	E.3: Cryptographic Parameter Override . . . . .	11
11.6.4	E.4: Server-to-Server Privilege Escalation . . . . .	12
<b>12</b>	<b>External Security Notes</b>	<b>12</b>
12.1	Deployment Recommendations . . . . .	12
12.2	Known Limitations . . . . .	12
12.3	Integration Considerations . . . . .	12
<b>13</b>	<b>Verification and Testing Plan</b>	<b>12</b>
13.1	Security Test Suite . . . . .	12
13.2	Code Review Process . . . . .	12
13.3	Regression Testing . . . . .	12
<b>14</b>	<b>Document Maintenance</b>	<b>12</b>
14.1	Review Schedule . . . . .	12
14.2	Change Process . . . . .	12
14.3	Version History . . . . .	12

# **1 Introduction**

## **1.1 Document Purpose**

## **1.2 System Overview**

# **2 Scoping**

## **2.1 In Scope**

## **2.2 Out of Scope**

# **3 Use Scenarios**

## **3.1 Primary Use Case**

## **3.2 Anti-Scenarios**

# **4 Dependencies**

## **4.1 External Libraries**

- galois:
- numpy:
- Python standard library:

## **4.2 System Dependencies**

- Network stack:
- File system:
- Operating system:

# **5 Implementation Assumptions**

- placeholder
- placeholder
- placeholder
- placeholder
- placeholder

## **6 Trust Levels**

- 6.1 Administrator**
- 6.2 Authenticated Client**
- 6.3 Storage Server**
- 6.4 Untrusted Network**

## **7 Entry Points**

### **7.1 Client API**

- **Store operation:**
- **Retrieve operation:**
- **Verify operation:**

### **7.2 Inter-Server Communication**

- **Fingerprint exchange:**
- **Fragment retrieval:**

### **7.3 Storage Subsystem**

- **Fragment write:**
- **Fragment read:**
- **Fingerprint storage:**

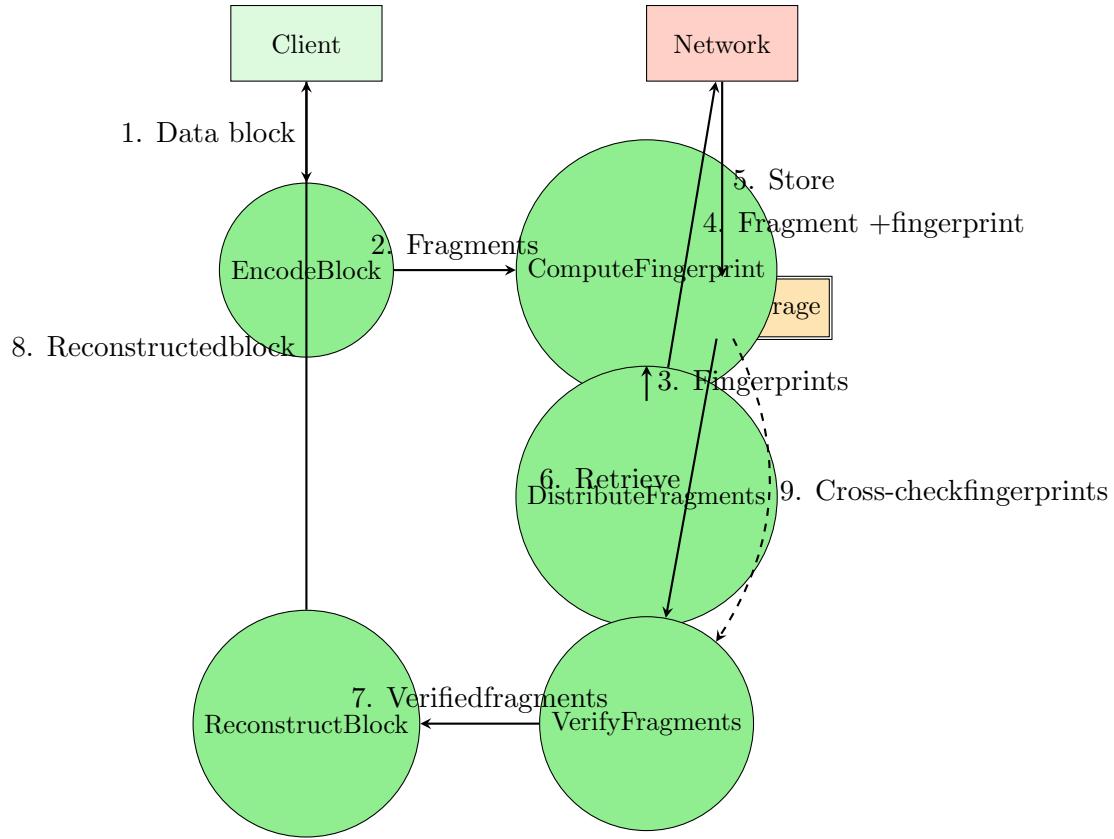


Figure 1: High-level data flow diagram for veri-store store and retrieve operations.

## **8 Protected Assets**

- 8.1 Data Blocks**
- 8.2 Erasure-Coded Fragments**
- 8.3 Homomorphic Fingerprints**
- 8.4 System Resources**

## **9 Data Flow Diagram**

- 9.1 DFD Component Descriptions**
  - 9.1.1 Client**
  - 9.1.2 Encode Block**
  - 9.1.3 Compute Fingerprint**
  - 9.1.4 Distribute Fragments**
  - 9.1.5 Network**
  - 9.1.6 Fragment Storage**
  - 9.1.7 Verify Fragments**
  - 9.1.8 Reconstruct Block**

## **10 Threat Analysis: STRIDE**

- 10.1 Spoofing**
  - 10.1.1 S.1: Client Impersonation**
  - 10.1.2 S.2: Server Impersonation**
  - 10.1.3 S.3: Fingerprint Source Forgery**
- 10.2 Tampering**
  - 10.2.1 T.1: Fragment Corruption in Storage**
  - 10.2.2 T.2: Fragment Modification in Transit**
  - 10.2.3 T.3: Fingerprint Tampering**
  - 10.2.4 T.4: Erasure Code Parameter Manipulation**
- 10.3 Repudiation**
  - 10.3.1 R.1: Anonymous Data Storage**
  - 10.3.2 R.2: Fragment Deletion Without Logging**
  - 10.3.3 R.3: Untrackable Verification Failures**
- 10.4 Information Disclosure**
  - 10.4.1 I.1: Fragment Eavesdropping**
  - 10.4.2 I.2: Storage Server Data Access** 7
  - 10.4.3 I.3: Fingerprint Analysis**
  - 10.4.4 I.4: Error Message Information Leakage**

- Resolution:
- Owner:
- Testing:

#### **11.1.2 S.2: Server Impersonation**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.1.3 S.3: Fingerprint Source Forgery**

- Status:
- Resolution:
- Owner:
- Testing:

### **11.2 Tampering Threat Resolutions**

#### **11.2.1 T.1: Fragment Corruption in Storage**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.2.2 T.2: Fragment Modification in Transit**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.2.3 T.3: Fingerprint Tampering**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.2.4 T.4: Erasure Code Parameter Manipulation**

- Status:
- Resolution:
- Owner:
- Testing:

### **11.3 Repudiation Threat Resolutions**

#### **11.3.1 R.1: Anonymous Data Storage**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.3.2 R.2: Fragment Deletion Without Logging**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.3.3 R.3: Untrackable Verification Failures**

- Status:
- Resolution:
- Owner:
- Testing:

### **11.4 Information Disclosure Threat Resolutions**

#### **11.4.1 I.1: Fragment Eavesdropping**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.4.2 I.2: Storage Server Data Access**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.4.3 I.3: Fingerprint Analysis**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.4.4 I.4: Error Message Information Leakage**

- Status:
- Resolution:
- Owner:
- Testing:

### **11.5 Denial of Service Threat Resolutions**

#### **11.5.1 D.1: Storage Exhaustion**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.5.2 D.2: Fragment Unavailability**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.5.3 D.3: Verification Flooding**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.5.4 D.4: Network Bandwidth Exhaustion**

- Status:
- Resolution:
- Owner:
- Testing:

### **11.6 Elevation of Privilege Threat Resolutions**

#### **11.6.1 E.1: Code Injection via Malformed Input**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.6.2 E.2: Verification Bypass**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.6.3 E.3: Cryptographic Parameter Override**

- Status:
- Resolution:
- Owner:
- Testing:

#### **11.6.4 E.4: Server-to-Server Privilege Escalation**

- Status:
- Resolution:
- Owner:
- Testing:

## **12 External Security Notes**

### **12.1 Deployment Recommendations**

### **12.2 Known Limitations**

### **12.3 Integration Considerations**

## **13 Verification and Testing Plan**

### **13.1 Security Test Suite**

### **13.2 Code Review Process**

### **13.3 Regression Testing**

## **14 Document Maintenance**

### **14.1 Review Schedule**

### **14.2 Change Process**

### **14.3 Version History**

- **Version 0.1** (February 16, 2026): Initial draft - high-level security model with component stubs