PreTech-NIDS Database Schema Documentation

# Database Overview

The PreTech-NIDS system employs MongoDB as the primary database management system, a document-based NoSQL database particularly suitable for handling large volumes of unstructured data and real-time data streams generated by network intrusion detection systems.

#### **4.3.3.1 Users Collection**

*Table 29: Users Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| uid | string | NOT NULL | User unique identifier |
| display\_name | string | NOT NULL | User display name |
| email | string | NOT NULL | User email address |
| phone\_number | string | NOT NULL | User phone number |
| profile\_pic | string | - | Profile picture URL path |
| role | string | NOT NULL | User role (admin, analyst, user) |
| created\_time | timestamp | NOT NULL | User account creation timestamp |
| last\_login | timestamp | - | Last login time |
| is\_active | boolean | NOT NULL | Account activation status |

#### **4.3.3.2 Detection Reports Collection**

*Table 30: Detection Reports Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| model | string | NOT NULL | Machine learning model name used |
| input | array[float] | NOT NULL | Input feature vector (77-dimensional features) |
| output | object | NOT NULL | Model prediction results and confidence |
| timestamp | string | NOT NULL | Detection timestamp (ISO format) |
| type | string | NOT NULL | Detection type (manual\_testing/real\_time\_detection) |
| interface | string | - | Network interface name |
| result | object | NOT NULL | Prediction result details (prediction, probability) |
| src\_ip | string | - | Source IP address from packet |
| dst\_ip | string | - | Destination IP address from packet |
| dst\_port | integer | - | Destination port number |
| protocol | string | - | Protocol type (TCP/UDP/ICMP) |

#### **4.3.3.3 Alerts Collection**

*Table 31: Alerts Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| rule\_id | string | NOT NULL | Alert rule identifier |
| alert\_type | string | NOT NULL | Alert type (threat\_detected, anomaly\_detected, etc.) |
| level | string | NOT NULL | Alert level (critical, high, medium, low, info) |
| title | string | NOT NULL | Alert title |
| message | string | NOT NULL | Alert detailed information |
| source\_ip | string | - | Source IP address |
| destination\_ip | string | - | Destination IP address |
| target\_port | integer | - | Target port number |
| protocol | string | - | Protocol type |
| model | string | - | Model name that triggered the alert |
| confidence | float | - | Detection confidence |
| timestamp | string | NOT NULL | Alert generation timestamp |
| acknowledged | boolean | NOT NULL | Whether acknowledged |
| acknowledged\_by | string | - | Acknowledging user ID |
| resolved | boolean | NOT NULL | Whether resolved |
| resolved\_by | string | - | Resolving user ID |

#### **4.3.3.4 Alert Rules Collection**

*Table 32: Alert Rules Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| id | string | NOT NULL | Rule unique identifier |
| name | string | NOT NULL | Rule name |
| description | string | NOT NULL | Rule description |
| alert\_type | string | NOT NULL | Alert type |
| conditions | object | NOT NULL | Trigger condition configuration |
| actions | array[string] | NOT NULL | Action list to execute |
| enabled | boolean | NOT NULL | Whether rule is enabled |
| threshold | float | - | Trigger threshold |
| time\_window | integer | - | Time window (minutes) |
| created\_at | string | NOT NULL | Rule creation time |
| updated\_at | string | NOT NULL | Rule update time |

#### **4.3.3.5 Alert History Collection**

*Table 33: Alert History Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| alert\_id | string | NOT NULL | Original alert ID |
| action | string | NOT NULL | Action performed (acknowledge, resolve, escalate, etc.) |
| user\_id | string | NOT NULL | User ID who performed the action |
| timestamp | string | NOT NULL | Action execution time |
| notes | string | - | Notes information |
| previous\_state | object | NOT NULL | State before operation |
| new\_state | object | NOT NULL | State after operation |

#### **4.3.3.6 Attack Locations Collection**

*Table 34: Attack Locations Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| timestamp | string | NOT NULL | Attack detection timestamp |
| source\_ip | string | NOT NULL | Source IP address of the attack |
| location | object | NOT NULL | Geographic location information |
| attack\_details | object | NOT NULL | Attack details including model and prediction |
| country | string | NOT NULL | Country name |
| country\_code | string | NOT NULL | Country code (ISO format) |
| latitude | float | NOT NULL | Latitude coordinate |
| longitude | float | NOT NULL | Longitude coordinate |

#### **4.3.3.7 Geo Cache Collection**

*Table 35: Geo Cache Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| ip | string | NOT NULL | IP address |
| location\_data | object | NOT NULL | Geographic location data |
| cached\_at | string | NOT NULL | Cache timestamp |

#### **4.3.3.8 PCAP Analyses Collection**

*Table 36: PCAP Analyses Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| filename | string | NOT NULL | PCAP filename |
| file\_hash | string | NOT NULL | File MD5 hash value |
| file\_size | integer | NOT NULL | File size (bytes) |
| total\_packets | integer | NOT NULL | Total packet count |
| packet\_analysis | object | NOT NULL | Packet analysis results |
| threat\_analysis | object | NOT NULL | Threat analysis and assessment |
| timestamp | string | NOT NULL | Analysis completion time |
| processing\_time | float | NOT NULL | Processing time (seconds) |
| status | string | NOT NULL | Analysis status (completed, failed, processing) |

#### **4.3.3.9 PCAP Reports Collection**

*Table 37: PCAP Reports Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| analysis\_id | string | NOT NULL | Associated analysis ID |
| report\_type | string | NOT NULL | Report type (summary, detailed, threat\_analysis) |
| content | object | NOT NULL | Report content |
| generated\_at | string | NOT NULL | Report generation time |
| format | string | NOT NULL | Report format (json, pdf, html) |

#### **4.3.3.10 Password Resets Collection**

*Table 38: Password Resets Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| email | string | NOT NULL | User email address |
| token | string | NOT NULL | Reset token |
| expires\_at | timestamp | NOT NULL | Expiration time |
| used | boolean | NOT NULL | Whether used |
| created\_at | timestamp | NOT NULL | Creation time |

#### **4.3.3.11 Registration Verifications Collection**

*Table 39: Registration Verifications Collection Database Schema Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Constraints** | **Description** |
| \_id | ObjectId | Primary Key (PK) | MongoDB auto-generated unique identifier |
| email | string | NOT NULL | User email address |
| otp\_code | string | NOT NULL | One-time verification code |
| expires\_at | timestamp | NOT NULL | Verification code expiration time |
| verified | boolean | NOT NULL | Whether verified |
| created\_at | timestamp | NOT NULL | Creation time |
| verified\_at | timestamp | - | Verification completion time |