To simulate a real-world deployment of the network attack detection system, we built a test environment with:

* **4 hosts** (1 for visualization, 3 for user group simulation)
* **1 switch**
* **1 high-performance server**

The network topology is shown in fig. 1.

* **High-performance server**: Handles core computation tasks, including training the NAD-GNN model and running detection. It processes network traffic efficiently and performs deep learning inference to identify potential attacks. (See table 1 for details.)
* **Visualization platform**: Displays detection results in real time, providing security administrators with an intuitive view of threats. (See table 2 for details.)

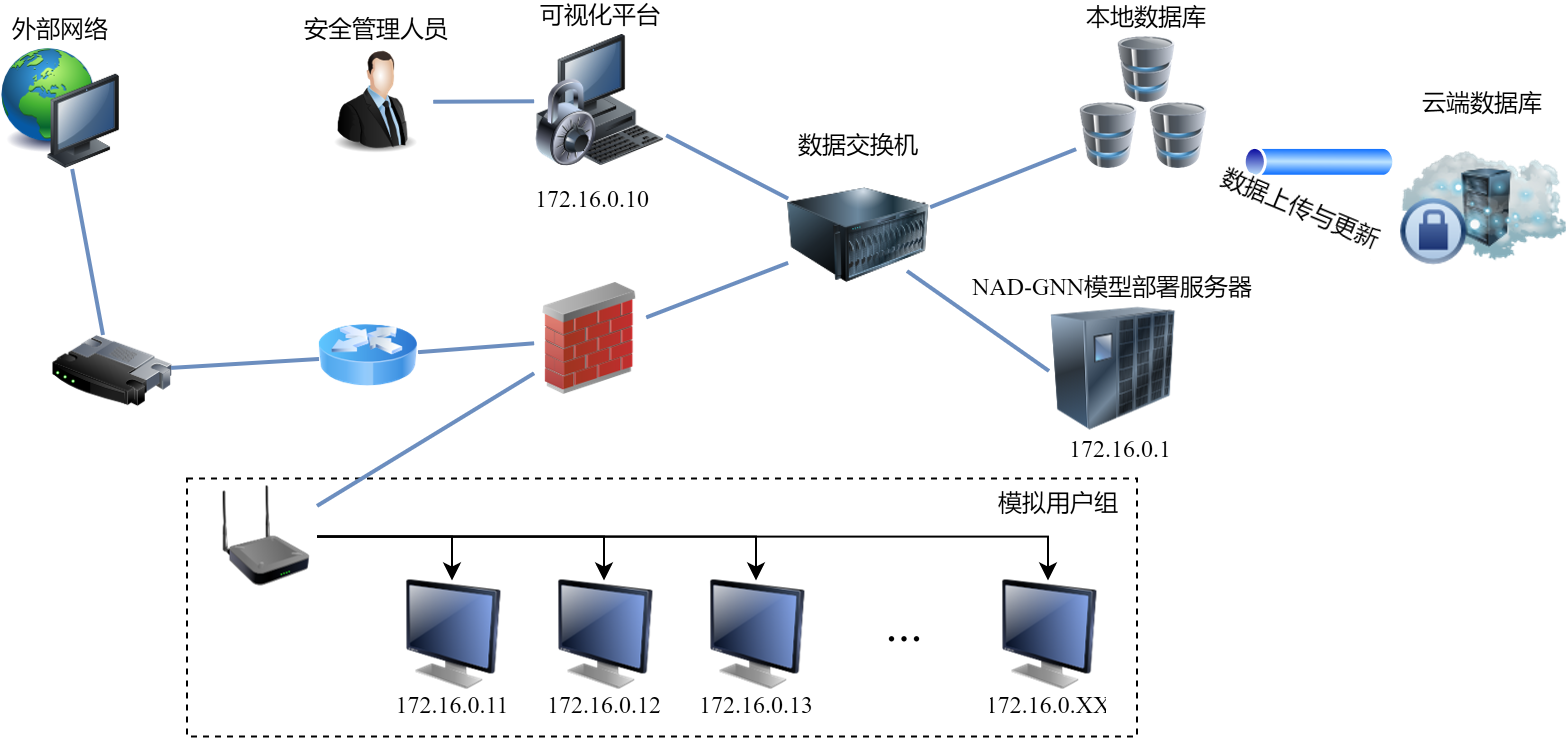


fig. 1 Diagram of Experimental Network Topology

**Platform Login Interface**

Fig. 2 shows the login page of the platform.

* **Authentication**: Administrators log in with a username and password to ensure that only authorized users can access the system.
* **Access control**: After a successful login, the system loads different monitoring modules based on the administrator’s permissions, providing real-time attack detection data.
* **Multi-language support**: The login page supports multiple languages, making the platform accessible to users from different regions.

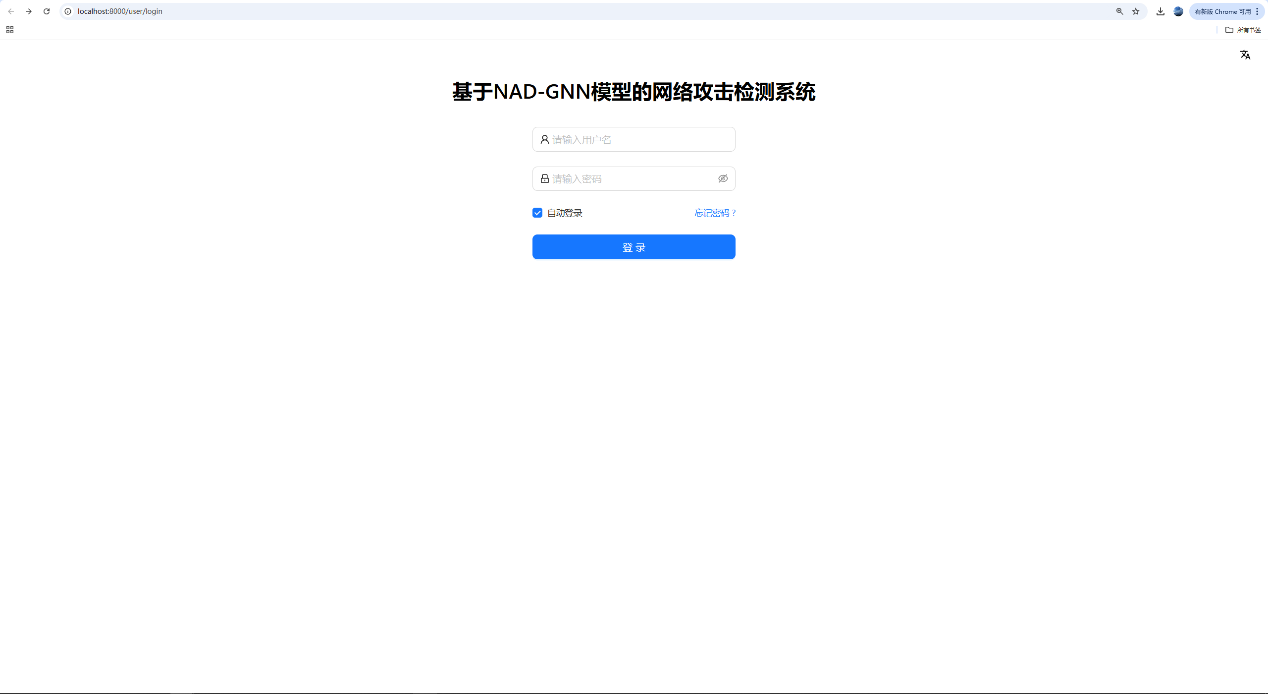


fig. 2 Screenshot of the network attack detection system interactive platform interface

table 1 Experimental Host Environment

|  |  |
| --- | --- |
| Main Module | Configuration |
| CPU | Intel(R) Xeon(R) Silver 4210R @ 2.40GHz |
| GPU | GeForce RTX 3090 |
| System | Linux（Ubuntu 20.04.1 LTS） |
| System architecture | 64-bit |
| Remote development tools | FinalShell 2.4.5 |

table 2 Visualization Platform Environment

|  |  |
| --- | --- |
| Main Module | Configuration |
| CPU | 12th Gen Intel(R) Core(TM) i5-12500 @ 3.00GHz |
| GPU | GeForce RTX 3050 |
| System | Windows 11 |
| System architecture | 64-bit |
| Remote development tools | MySQL 5.6 |

**Example of Local Database Table**

Fig. 3 shows an example table, **Phishing\_InfoGain**, stored in the local database system. This table contains information for identifying and analyzing phishing attacks. Each row represents a network traffic sample, while the columns store various traffic features such as domain\_token\_count, avgdomainintokenlen, tld, and pathurlRatio. These features capture statistical information about domain names, URL paths, character sequences, and symbol counts.

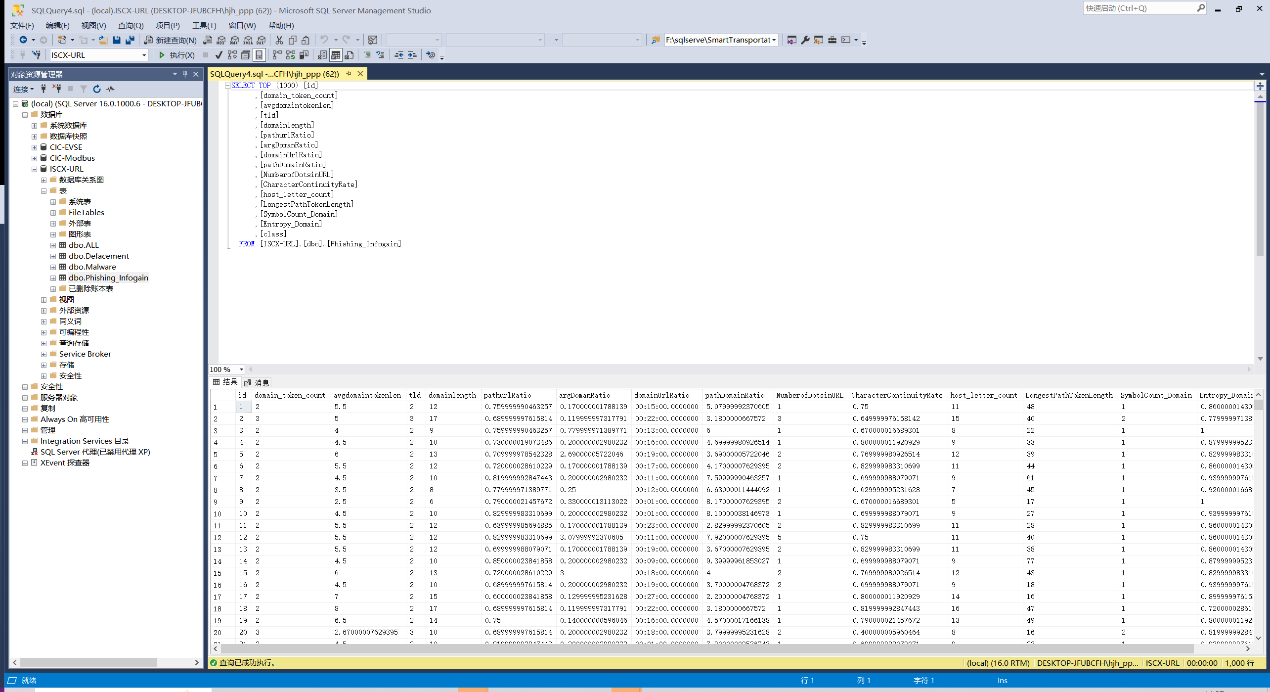


fig. 3 Screenshot of database system

**Visualization Interface**

Fig. 4 shows the visualization interface of the NAD-GNN–based attack detection platform. It provides administrators with information on detected anomalous traffic, attack types, and severity levels, and also supports querying and analyzing historical data.



fig. 4 Screenshot of the visualization platform interface for the network attack detection system