

Table of contents

1. SYSTEM REQUIREMENTS:	2
2. RUNNING THE APPLICATION:	2
3. USING THE APPLICATION	2
3.1 CONNECTING TO THE DATABASE	2
3.2 SETTING SECURITY LEVELS	3
3.3 SELECTING THE PHASE	4
3.4 SPYING THE DATABASE	4
3.5 CHANGING THE SETTINGS	5
3.6 SIMULATION ENVIRONMENT	6

1. System Requirements:

- Windows XP Service Pack 2 or higher
- Oracle 10g Express Edition 2005
- .NET Framework 2.0

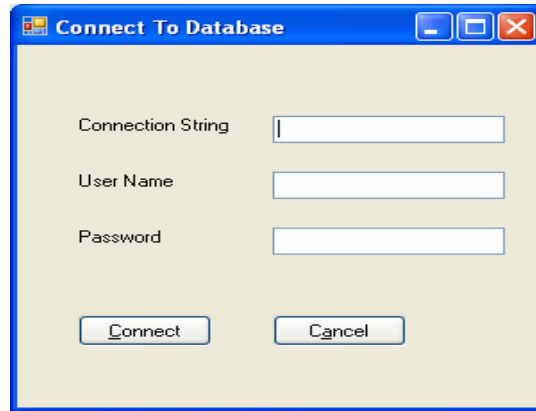
2. Running the Application:

The application doesn't come as a package and hence need not be installed separately. If all the system requirements are in place, then the application can be run by running the .exe file. The following sections offer help by illustrating the use of the application.

3. Using the Application

3.1 Connecting to the database

The “**To Database**” Option from the **Connect** menu can be used to Connect to the database. The Connect form opens up in which the user (Administrator) can enter the **connection string, username and password** to login to the database. If left blank the system takes the default connection string for that particular database. The login must have administrative privileges in order to perform other tasks with the application

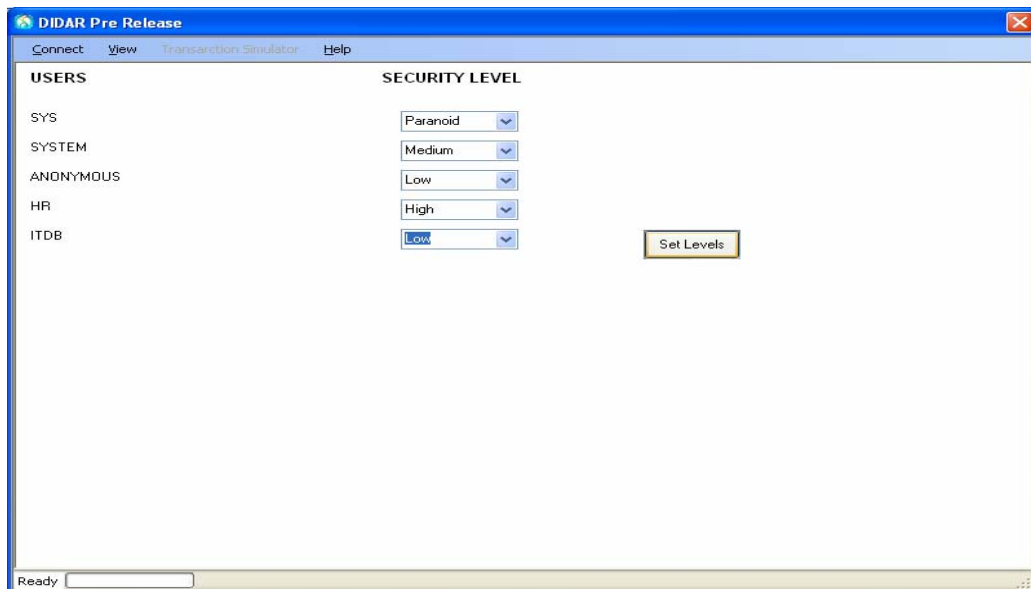


A Windows-style dialog box titled "Connect To Database". It contains three input fields: "Connection String", "User Name", and "Password". Below these fields are two buttons: "Connect" and "Cancel".

Fig 1: Connect Form

3.2 Setting Security Levels

Once the administrator logs in, he is presented with a list of users who have an open account in the database. He may choose to set security permissions for these users, to monitor their transactions. He may choose between “**Low**”, “**Medium**”, “**High**” and “**Paranoid**” security levels for each user. The default security settings are “**High**” for all the users



The main application window titled "DIDAR Pre Release". It has a menu bar with "Connect", "View", "Transaction Simulator", and "Help". The main area is divided into two columns: "USERS" and "SECURITY LEVEL".

USERS	SECURITY LEVEL
SYS	Paranoid
SYSTEM	Medium
ANONYMOUS	Low
HR	High
ITDB	Low

Below the table is a "Set Levels" button. The status bar at the bottom shows "Ready".

Fig 2: MainScreen

3.3 Selecting the Phase

After setting the security levels, you can select the phase that you want to work with i.e. **“Learning”** or **“Detection”**. This can be done by selecting the appropriate option from the **Options menu** in the **View** menu

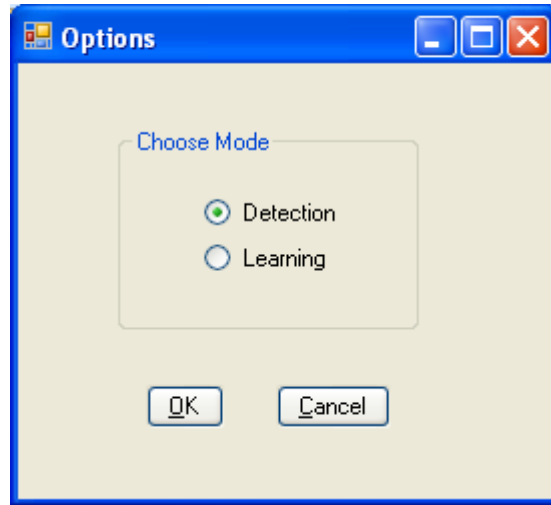


Fig 3: Options Form

3.4 Spying the Database

The **“Spy the Database”** option provides you an opportunity to see what is happening inside the database. It presents the list of all executing queries in the database and can be selected by choosing the **“Spy the Database”** option from the **“View”** menu.

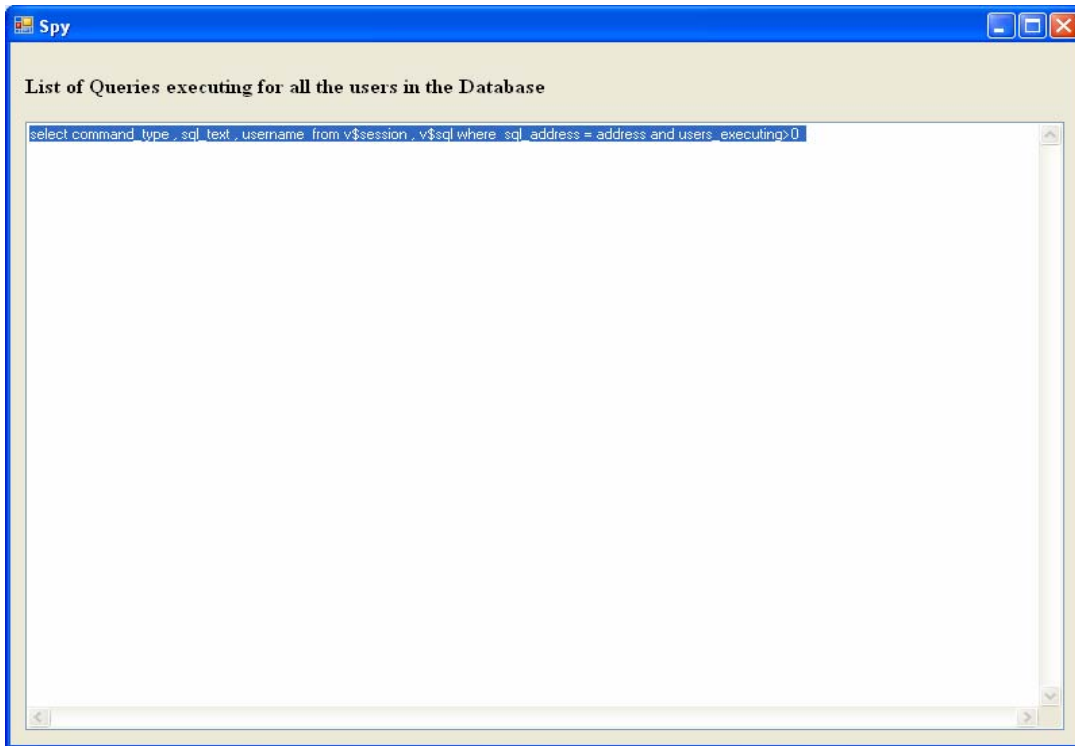


Fig 4: Spying the Database

3.5 Changing the Settings

The “**Settings**” option from the “**View**” menu lets you change the default settings of the application. The **timer interval** lets you specify the interval between refreshing the list of currently executing queries. The **Risk settings** lets you specify the limits for classification of intrusions into different levels of risk i.e. “**Low**”, “**Medium**” and “**High**”.

The image shows a Windows-style dialog box titled "Settings". It has a blue title bar with standard minimize, maximize, and close buttons. The main content area is divided into two sections. The first section, labeled "Settings", contains a "Refresh time interval" set to "5000" milliseconds, with a unit label "MilliSeconds" and a button labeled "Auto Refresh Security Levels". The second section, labeled "Risk and Security settings", contains the instruction "Set the no. of Tables affected in intrusion for Risk classification" followed by three rows of settings: "High Risk >=" with a value of "6", "Medium Risk <=" with a value of "4", and "Low Risk >=" with a value of "2". At the bottom right of the dialog are "OK" and "Cancel" buttons. A red text note at the bottom states: "NOTE : The Values here Indicate Default Values. Change them and click OK for the new settings to take effect".

Fig 5: Settings Form

Clicking on the “Auto Refresh Security Levels” automatically changes the user security levels based on the intrusions and the risk associated with each intrusion for each user and their overall threat.

3.6 Simulation Environment

We also provide a transaction simulator to simulate random fingerprints of transactions. The Transaction Simulator can be used to test the learning and the detection capabilities of the system. The transaction simulator can be turned on/off from the **Transaction Simulator** menu option.

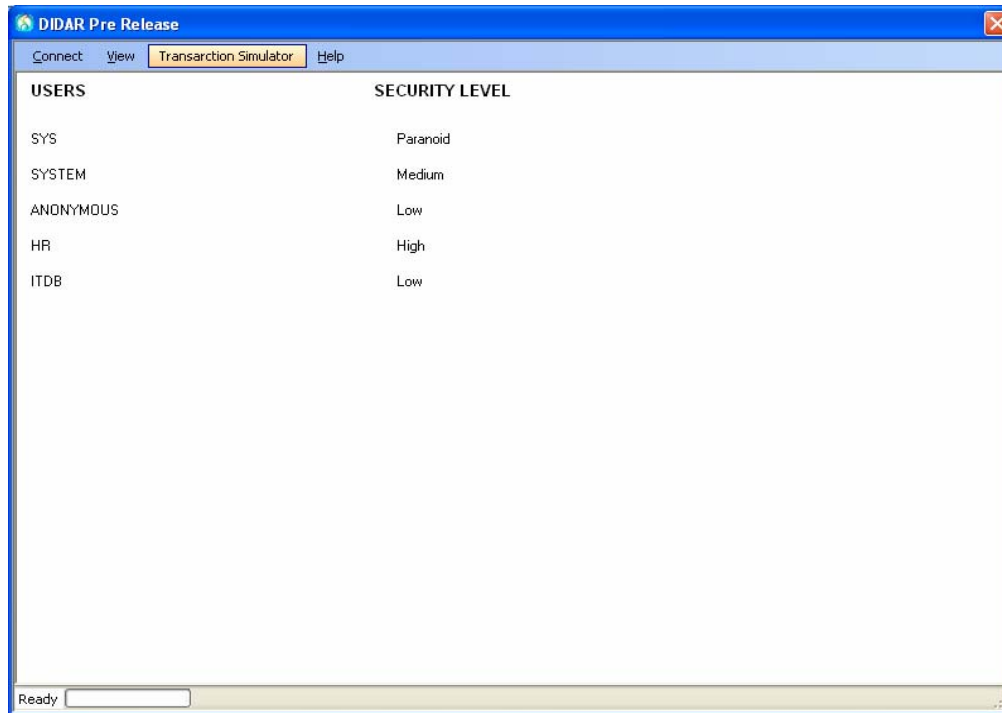


Fig 6: Transaction Simulator Menu item