TRƯỜNG ĐẠI HỌC KINH TẾ

Khoa Thống kê – Tin học

--🙡🕮🙣--



**BÁO CÁO**

Hệ Quản trị Cơ sở dữ liệu

Giảng viên hướng dẫn: Cao Thị Nhâm

Nhóm 16:

1. Lê Tâm Hạnh 43K21
2. Nguyễn Thị Quý Huyên 43K21

*Đà Nẵng, tháng 11 năm 2019*

**MỤC LỤC**

[1. Hóa đơn bán hàng 3](#_Toc24307828)

[2. Thiết kế cơ sở dữ liệu 3](#_Toc24307829)

[2.1. Thiết kế cơ sở dữ liệu Mức khái niệm 3](#_Toc24307830)

[2.2. Thiết kế cơ sở dữ liệu Mức logic 5](#_Toc24307831)

[2.3. Thiết kế cơ sở dữ liệu Mức vật lý 6](#_Toc24307832)

[3. Xây dựng cơ sở dữ liệu 7](#_Toc24307833)

[4. Xác định và tạo các index cho các thuộc tín 9](#_Toc24307834)

[5. Xây dựng cơ chế bảo mật 10](#_Toc24307835)

[6. Xây dựng cơ chế backup dữ liệu 11](#_Toc24307836)

[7. Phát triển ứng dụng 13](#_Toc24307837)

[7.1. Form Đăng nhập 13](#_Toc24307838)

[7.2. Form Quản lý Bán hàng 14](#_Toc24307839)

[7.3. Form Quản lý Hàng 16](#_Toc24307840)

[7.4. Form Quản lý Khách: 17](#_Toc24307841)

[7.5. Form Quản lý Hóa đơn 18](#_Toc24307842)

[7.6. Form Quản lý Chi tiết Hóa đơn 19](#_Toc24307843)

[8. Giải quyết vấn đề dữ liệu lớn 20](#_Toc24307844)

[9. Phòng chống SQL Injection 20](#_Toc24307845)

DANH SÁCH HÌNH ẢNH

[Hình 1.1 Hóa đơn bán hàng của Lyn's Clothes & Accessories 3](#_Toc24307853)

[Hình 2.1 Mô hình E-R 4](#_Toc24307854)

[Hình 2.2 Sơ đồ quan hệ 5](#_Toc24307855)

[Hình 2.3 Thiết kế bảng Hàng 6](#_Toc24307856)

[Hình 2.4 Thiết kế bảng Khách 6](#_Toc24307857)

[Hình 2.5 Thiết kế bảng Hóa đơn 6](#_Toc24307858)

[Hình 2.6 Thiết kế bảng Chi tiết Hóa đơn 6](#_Toc24307859)

[Hình 3.1 Xây dựng bảng Hàng 7](#_Toc24307860)

[Hình 3.2 Xây dựng bảng Khách 7](#_Toc24307861)

[Hình 3.3 Xây dựng bảng Hóa đơn 8](#_Toc24307862)

[Hình 3.4 Xây dựng bảng Chi tiết Hóa đơn 8](#_Toc24307863)

[Hình 4.1 Tạo Index cho CSDL 9](#_Toc24307864)

[Hình 5.1 Bảng Phân quyền người dùng 10](#_Toc24307865)

[Hình 5.2 Mã hóa dữ liệu bảng Khách 10](#_Toc24307866)

[Hình 5.3 Bảng đã được mã hóa 11](#_Toc24307867)

[Hình 5.4 Hàm giải mã 11](#_Toc24307868)

[Hình 6.1 Maintenance Plans 12](#_Toc24307869)

[Hình 6.2 SQL Server Agents Job 13](#_Toc24307870)

[Hình 6.3 File Backup 13](#_Toc24307871)

[Hình 7.1 Form Đăng nhập 13](#_Toc24307872)

[Hình 7.2 Form Quản lý Bán hàng (Admin) 14](#_Toc24307873)

[Hình 7.3 Form Quản lý Bán hàng (User) 15](#_Toc24307874)

[Hình 7.4 Form Quản lý Hàng 16](#_Toc24307875)

[Hình 7.5 Form Quản lý Khách hàng 17](#_Toc24307876)

[Hình 7.6 Form Quản lý Hóa đơn 18](#_Toc24307877)

[Hình 7.7 Form Quản lý Chi tiết Hóa đơn 19](#_Toc24307878)

[Hình 9.1 Thay thế các ký tự đặc biệt 20](#_Toc24307879)

[Hình 9.2 Kiểm tra 'OR 1=1-- 21](#_Toc24307880)

# Hóa đơn bán hàng



Hình 1.1 Hóa đơn bán hàng của Lyn's Clothes & Accessories

# Thiết kế cơ sở dữ liệu

## Thiết kế cơ sở dữ liệu Mức khái niệm

**❖ Bước 1: Chọn lọc thông tin**

Xây dựng ***Từ điển dữ liệu***

|  |  |  |
| --- | --- | --- |
| **Từ trong HSDL** | **Từ rõ nghĩa** | **Viết tắt** |
| Số phiếu | Mã hóa đơn | MaHD |
| Ngày | Ngày bán | NgayBan |
| In lúc | Thời gian bán | ThoiGian |
| Điểm tích lũy trên hóa đơn | Điểm tích lũy trên hóa đơn | DiemTL |
| Mã hàng | Mã hàng hóa | MaH |
| Mặt hàng | **Tên hàng** | **TenH** |
| Giá | Đơn giá | DonGia |
| CK% | Chiết khấu | ChietKhau |
| Tồn kho | Số lượng tồn kho | SLT |
| SL | Số lượng bán | SLB |
| T tiền | Thành tiền | ThanhTien |
| Tổng | Tổng tiền phải trả (Đã CK) | TongTT |
| Khách hàng | **Tên Khách hàng** | **TenKH** |
| Mã khách hàng | Mã khách hàng | MaKH |
| Số điện thoại | Số điện thoại khách hàng | SDT |
| Tổng tích lũy | Tổng điểm tích lũy | TongTL |

**❖ Bước 2: Xác định thực thể, thuộc tính**

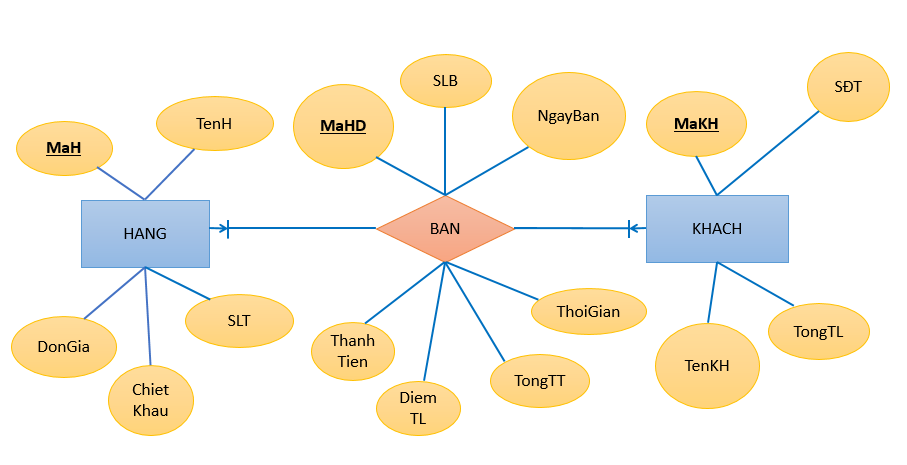
**KHACH**(**MaKH,** TenKH, SDT, TongTL)

**HANG**(**MaH**, TenH, DonGia, ChietKhau, SLT)

**❖ Bước 3: Xác định quan hệ**

**BÁN:** Bao gồm các thuộc tính còn lại trong từ điển

**❖ Bước 4: Vẽ ERD**

****

Hình 2.1 Mô hình E-R

## Thiết kế cơ sở dữ liệu Mức logic

**❖ Chuyển thực thể, thu được**

**KHACH**(**MaKH,** TenKH, SDT, TongTL)

**HANG**(**MaH**, TenH, DonGia, ChietKhau, SLT)

**❖ Chuyển quan hệ, thu được**

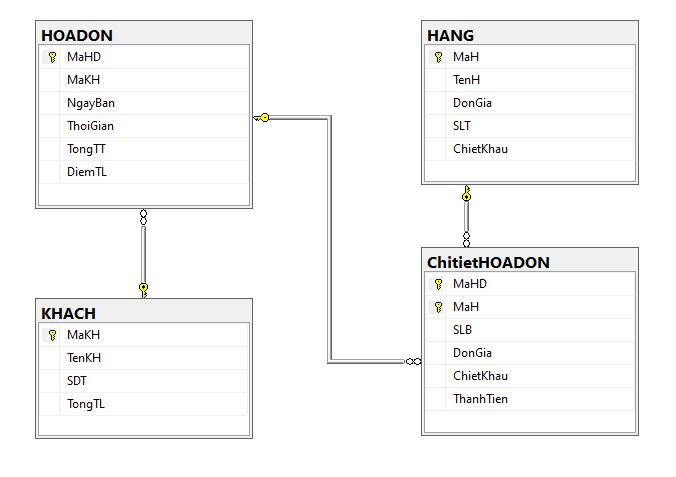
**BAN** (**MaK, MaH** NgayBan, ThoiGian, SLB, ThanhTien, TongTT, DiemTL)

**❖ Chuẩn hóa quan hệ BÁN, thu được**

**HOADON** (**MaHD,** MaKH, NgayBan, ThoiGian, TongTT, DiemTL)

**ChiTiet\_HD** (**MaHD, MaH**, SLB, DonGia, ChietKhau,ThanhTien)

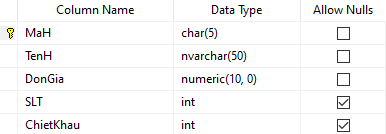
**❖ Vẽ sơ đồ quan hệ**



Hình 2.2 Sơ đồ quan hệ

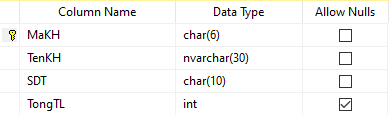
## Thiết kế cơ sở dữ liệu Mức vật lý

Bảng HÀNG



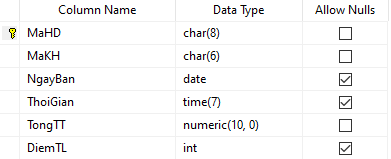
Hình 2.3 Thiết kế bảng Hàng

Bảng KHÁCH HÀNG



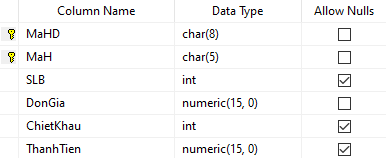
Hình 2.4 Thiết kế bảng Khách

Bảng HÓA ĐƠN



Hình 2.5 Thiết kế bảng Hóa đơn

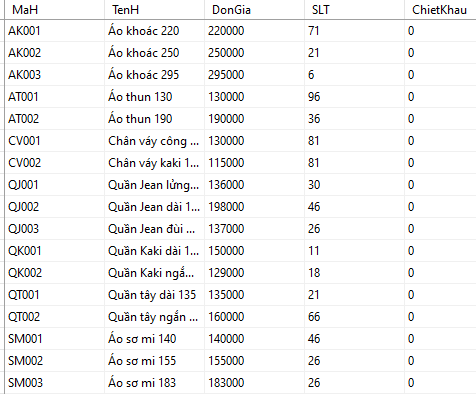
Bảng CHI TIẾT HÓA ĐƠN



Hình 2.6 Thiết kế bảng Chi tiết Hóa đơn

# Xây dựng cơ sở dữ liệu

Bảng HÀNG



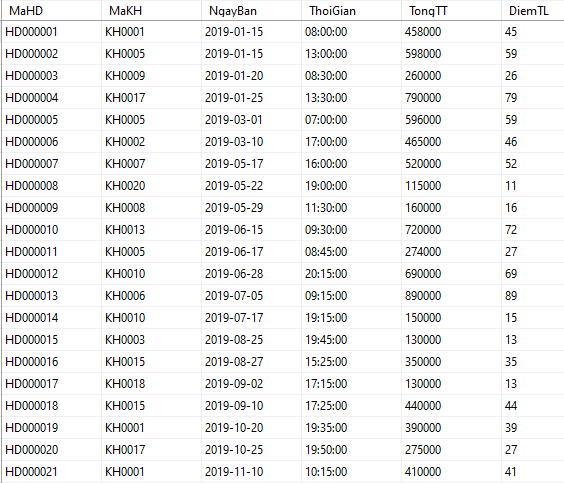
Hình 3.1 Xây dựng bảng Hàng

Bảng KHÁCH



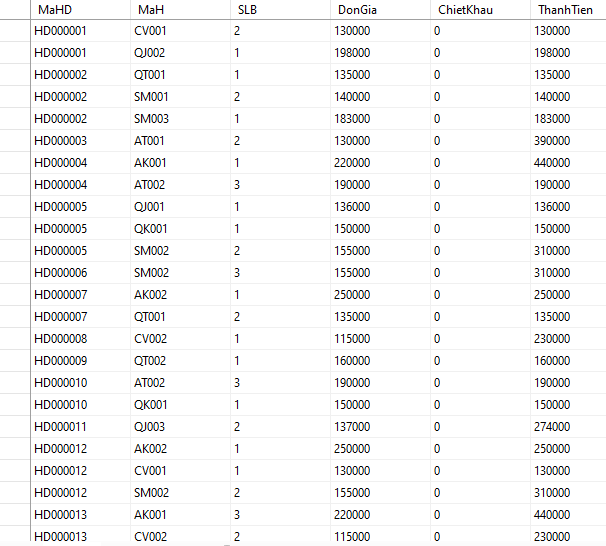
Hình 3.2 Xây dựng bảng Khách

Bảng HÓA ĐƠN



Hình 3.3 Xây dựng bảng Hóa đơn

Bảng Chi tiết HÓA ĐƠN



Hình 3.4 Xây dựng bảng Chi tiết Hóa đơn

# Xác định và tạo các index cho các thuộc tín

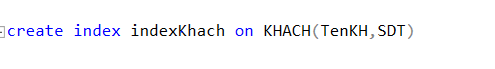
INDEX giúp tăng tốc các [truy vấn SELECT](https://quantrimang.com/lenh-select-trong-sql-143756) chứa các [mệnh đề WHERE](https://quantrimang.com/menh-de-where-trong-sql-143761) hoặc ORDER, nhưng nó làm chậm việc dữ liệu nhập vào với các [lệnh UPDATE](https://quantrimang.com/lenh-update-trong-sql-143766) và [INSERT](https://quantrimang.com/lenh-insert-trong-sql-143753). Các chỉ mục có thể được tạo hoặc xóa mà không ảnh hưởng tới dữ liệu.

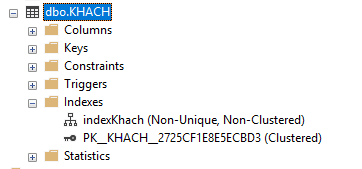
**Các kiểu index có trong SQL:**

* *Single-Column Index:* được tạo cho duy nhất 1 cột trong bảng. Cú pháp cơ bản như sau:
* *Unique Index:*là chỉ mục duy nhất, được sử dụng để tăng hiệu suất và đảm bảo tính toàn vẹn dữ liệu. Một chỉ mục duy nhất không cho phép chèn bất kỳ giá trị trùng lặp nào được chèn vào bảng. Cú pháp cơ bản như sau
* *Composite Index:* là chỉ mục kết hợp dành cho hai hoặc nhiều cột trong một bảng. Cú pháp cơ bản của nó như sau:
* *Implicit Index:* (Index ngầm định) là chỉ mục mà được tạo tự động bởi Database Server khi một bảng được tạo. Các Index ngầm định được tạo tự động cho các ràng buộc Primary key và các ràng buộc Unique.

Những trường hợp nên tránh sử dụng INDEX

* Không nên sử dụng trong các bảng nhỏ, ít bản ghi.
* Không nên sử dụng Index trong bảng mà các hoạt động UPDATE, INSERT xảy ra thường xuyên với tần suất lớn.
* Không nên sử dụng cho các cột mà chứa một số lượng lớn giá trị NULL.
* Không nên dùng Index cho các cột mà thường xuyên bị sửa đổi.

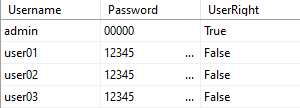


****

Hình 4.1 Tạo Index cho CSDL

# Xây dựng cơ chế bảo mật

❖ Xây dựng Bảng Account và phân quyền truy cập và chỉnh sửa dữ liệu ở cột UserRight



Hình 5.1 Bảng Phân quyền người dùng

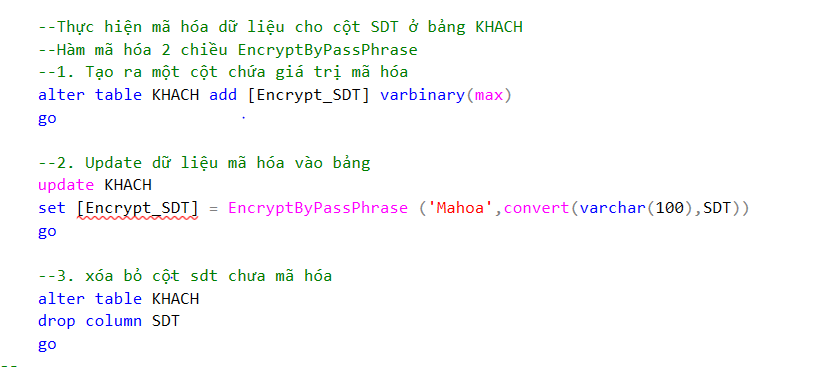
**+ True:**

* Người dùng được quyền truy cập Bảng KHÁCH
* Có quyền Tìm, Kiếm, Thêm, Sửa, Xóa ở tất cả các bảng

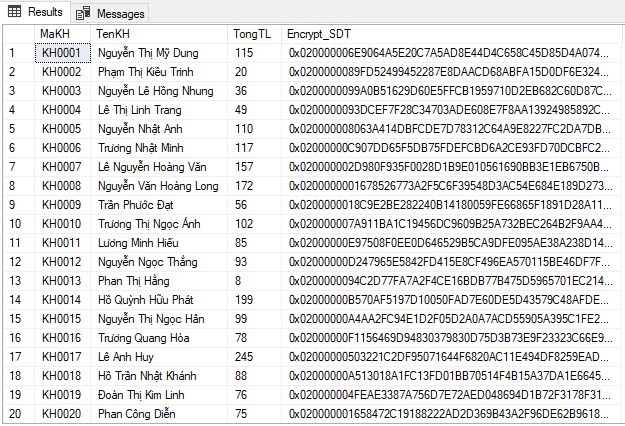
**+ False**

* Người dùng không được truy cập Bảng KHÁCH
* Chỉ có quyền Tìm Kiếm và Thêm dữ liệu ở các bảng còn lại

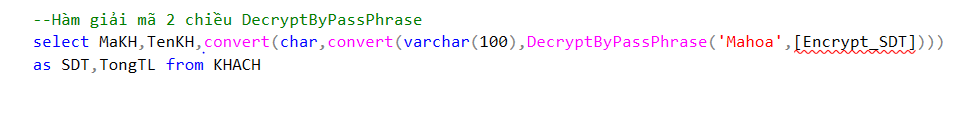
❖ Mã hóa dữ liệu



Hình 5.2 Mã hóa dữ liệu bảng Khách

****

Hình 5.3 Bảng đã được mã hóa

****

Hình 5.4 Hàm giải mã

# Xây dựng cơ chế backup dữ liệu

❖ Sao lưu và khôi phục dữ liệu là vấn đề rất quan trọng khi quản trị CSDL, đảm bảo cho dữ liệu không bị mất mát và nếu có sự cố xảy ra thì có thể khôi phục lại trạng thái của CSDL trước khi xảy ra sự cố. Công việc này phải dựa vào cơ chế Backup và Restore của các hệ QTCSDL, và để thực hiện tốt công việc này thì người quản trị dữ liệu phải có kịch bản sao lưu và khôi phục CSDL cho hệ thống một cách cẩn thận và chi tiết.

❖ Các loại sao lưu trong SQL Server cung cấp:

* ***Full Database Backups:*** Copy tất cả các file dữ liệu trong một database . Tất cả những user data và database objects như system tables, indexes, user-defined tables đều được backup.
* ***Differential Database Backups:*** Copy những thay đổi trong tất cả các file dữ liệu kể từ lần backup gần nhất.
* ***File or File Group Backups:*** Copy một data file đơn hay một nhóm file.
* ***Differential File or File Group Backups:*** Tương tự như *differential database backup* nhưng chỉ copy những thay đổi trong data file đơn hay một file group.
* ***Transaction Log Backups:*** Ghi nhận một cách thứ tự tất cả các giao dịch (transaction) chứa trong file transaction log kể từ lần transaction log backup gần nhất. Loại sao lưu này cho phép ta phục hồi dữ liệu trở ngược lại vào một thời điểm nào đó trong quá khứ mà vẫn đảm bảo tính đồng nhất (consistent).

❖ Trong lúc backup SQL Server cũng copy tất cả các hoạt động của database kể cả hoạt động xảy ra trong quá trình backup cho nên ta có thể backup trong khi SQL đang chạy mà không cần phải dừng lại.

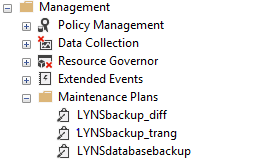
❖ Sử dụng tiện ích Jobs trong SQL Server Agent để lập lịch Backup dữ liệu.

* Tiện ích Jobs trong SQL Server Agent giúp cho việc tạo lịch backup dữ liệu được thực hiện tự động một cách dễ dàng . SQL Server Agent là module trong SQL Server dùng để tự động thực hiện các tác vụ về bảo trì và giám sát hệ thống.

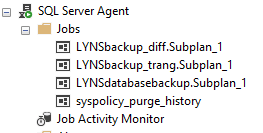
❖ Đối với cơ sở dữ liệu của nhóm:

Xây dựng kịch bản sao lưu và khôi phục dữ liệu cho cơ sở dữ liệu đã tạo như sau:

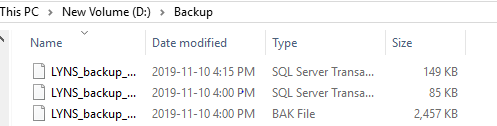
* Thực hiện **Full backup** dữ liệu vào 11h30 đêm mỗi ngày
* Thực hiện **Differential backup** vào các thời điểm (7h, 10h,13h,16h,19h,22h) (6 lần/ ngày)
* Thực hiện **Transaction log backup** 15 phút một lần vào các thời điểm 10’,25’,40’,55’ của mỗi giờ (4 lần/giờ).

****

Hình 6.1 Maintenance Plans

****

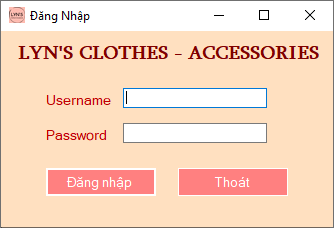
Hình 6.2 SQL Server Agents Job

****

Hình 6.3 File Backup

# Phát triển ứng dụng

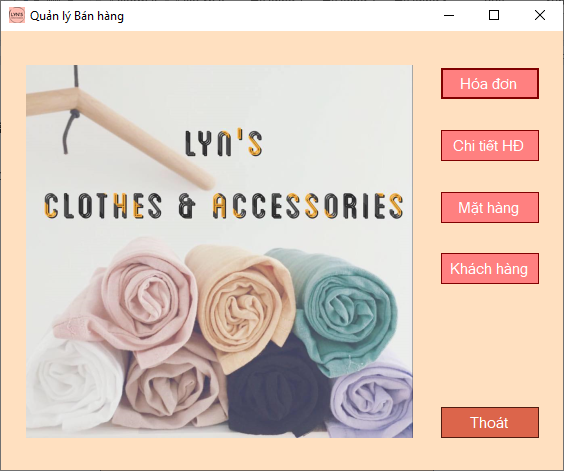
## Form Đăng nhập



Hình 7.1 Form Đăng nhập

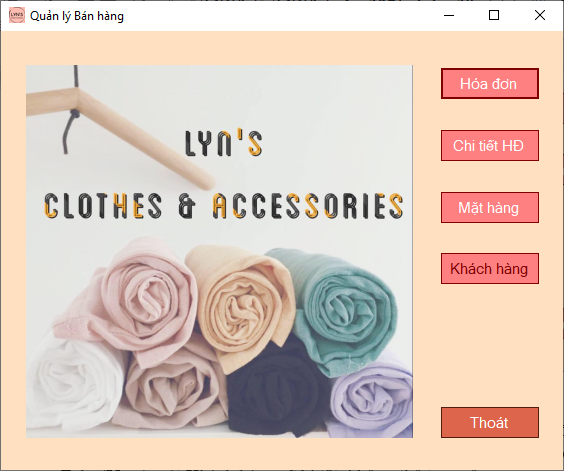
|  |  |
| --- | --- |
| **Công cụ** | **Sự kiện** |
| TextBox Username/Password | Nhập tên đăng nhập và mật khẩu của người dùng để đăng nhập và phân quyền sử dụng |
| Nút Đăng nhập | Nếu tên đăng nhập và mật khẩu chính xác thì khi Click/Enter sẽ truy cập vào form Quản lý, nếu sai sẽ báo lỗi và yêu cầu nhập lại |
| Nút Thoát | Kết thúc Chương trình |

## Form Quản lý Bán hàng



Hình 7.2 Form Quản lý Bán hàng (Admin)

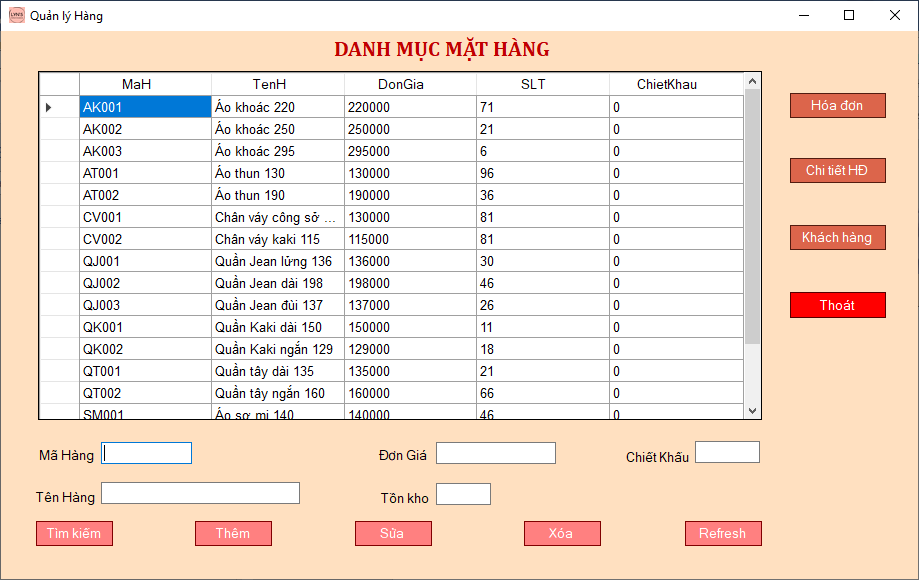
Với người dùng có **UserRight** = ***True*** (Admin), nút Khách hàng để truy cập bảng KHÁCH có thể kích hoạt được. Nhưng với người dùng có **UserRight** = ***False*** (User), nút Khách hàng sẽ bị tắt, không thể truy cập.



Hình 7.3 Form Quản lý Bán hàng (User)

|  |  |
| --- | --- |
| **Công cụ** | **Sự kiện** |
| Các Nút truy cập Bảng | Khi Click chuột sẽ mở Bảng tương ứng. Nếu UserRight của người dùng là False thì Nút Khách hàng sẽ bị vô hiệu hóa |
| Nút Thoát | Khi Click chuột trở về form Đăng nhập để đăng nhập bằng tài khoản khác hoặc kết thúc chương trình |

## Form Quản lý Hàng



Hình 7.4 Form Quản lý Hàng

|  |  |
| --- | --- |
| **Công cụ** | **Sự kiện** |
| Các TextBox để nhập giá trị | Nhập các giá trị tương ứng vào để thực hiện các chức năng Tìm Kiếm, Thêm, Sửa, Xóa |
| Nút Tìm kiếm | Khi Click vào thì các giá trị của Mã Hàng/Tên Hàng sẽ được dùng để Tìm kiếm và hiển thị trên DataGridView |
| Nút Thêm | Khi Click vào thì các giá trị đã nhập sẽ được dùng để thêm mới vào bảng HANG |
| Nút Sửa | Khi Click vào thì các giá trị đã nhập sẽ được dùng để cập nhật vào bảng HANG. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Xóa | Khi Click vào thì bản ghi có Mã Hàng/ Tên Hàng được nhập sẽ bị xóa trong bảng HANG. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Refresh | Khi Click vào thì form sẽ được load lại nếu trước đó sử dụng nút Tìm Kiếm |
| Các Nút truy cập Bảng khác | Khi Click vào thì sẽ mở các form khác và ẩn form hiện tại |

## Form Quản lý Khách:

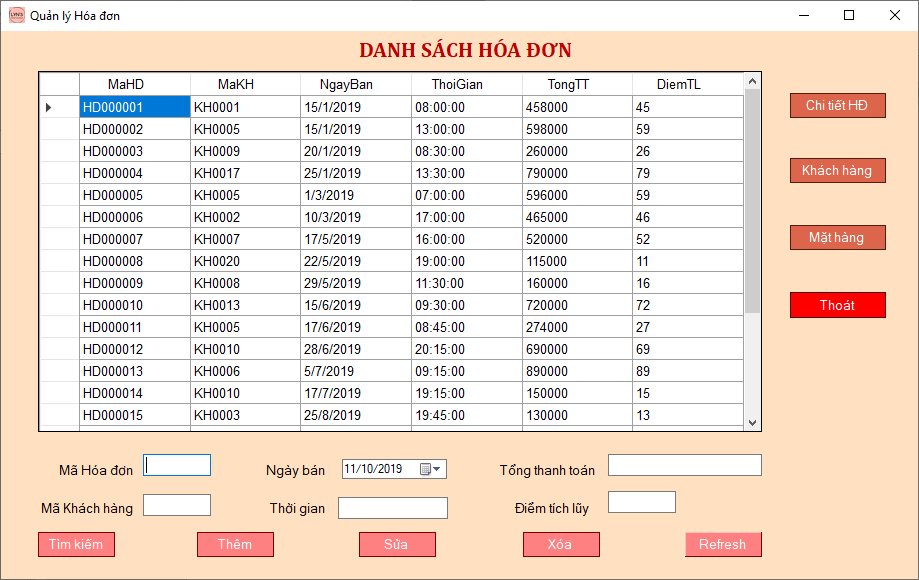
Chú ý: Form không thể truy cập với User (UserRight = False)



Hình 7.5 Form Quản lý Khách hàng

|  |  |
| --- | --- |
| **Công cụ** | **Sự kiện** |
| Các TextBox để nhập giá trị | Nhập các giá trị tương ứng vào để thực hiện các chức năng Tìm Kiếm, Thêm, Sửa, Xóa |
| Nút Tìm kiếm | Khi Click vào thì giá trị của Mã Khách hàng sẽ được dùng để Tìm kiếm và hiển thị trên DataGridView |
| Nút Thêm | Khi Click vào thì các giá trị đã nhập sẽ được dùng để thêm mới vào bảng KHACH |
| Nút Sửa | Khi Click vào thì các giá trị đã nhập sẽ được dùng để cập nhật vào bảng KHACH. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Xóa | Khi Click vào thì bản ghi có Mã Khách hàng được nhập sẽ bị xóa trong bảng KHACH. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Refresh | Khi Click vào thì form sẽ được load lại nếu trước đó sử dụng nút Tìm Kiếm |
| Các Nút truy cập Bảng khác | Khi Click vào thì sẽ mở các form khác và ẩn form hiện tại |

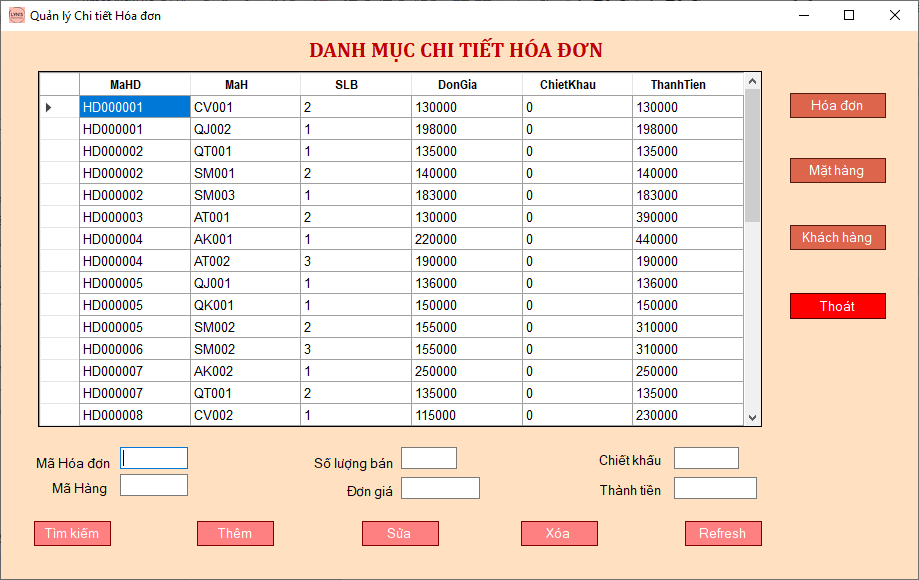
## Form Quản lý Hóa đơn



Hình 7.6 Form Quản lý Hóa đơn

|  |  |
| --- | --- |
| **Công cụ** | **Sự kiện** |
| Các TextBox để nhập giá trị | Nhập các giá trị tương ứng vào để thực hiện các chức năng Tìm Kiếm, Thêm, Sửa, Xóa |
| Nút Tìm kiếm | Khi Click vào thì giá trị của Mã Hóa đơn sẽ được dùng để Tìm kiếm và hiển thị trên DataGridView |
| Nút Thêm | Khi Click vào thì các giá trị đã nhập sẽ được dùng để thêm mới vào bảng HOADON |
| Nút Sửa | Khi Click vào thì các giá trị đã nhập sẽ được dùng để cập nhật vào bảng HOADON. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Xóa | Khi Click vào thì bản ghi có Mã Hóa đơn được nhập sẽ bị xóa trong bảng HOADON. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Refresh | Khi Click vào thì form sẽ được load lại nếu trước đó sử dụng nút Tìm Kiếm |
| Các Nút truy cập Bảng khác | Khi Click vào thì sẽ mở các form khác và ẩn form hiện tại |

## Form Quản lý Chi tiết Hóa đơn



Hình 7.7 Form Quản lý Chi tiết Hóa đơn

|  |  |
| --- | --- |
| **Công cụ** | **Sự kiện** |
| Các TextBox để nhập giá trị | Nhập các giá trị tương ứng vào để thực hiện các chức năng Tìm Kiếm, Thêm, Sửa, Xóa |
| Nút Tìm kiếm | Khi Click vào thì giá trị của Mã Hóa đơn + Mã Hàng sẽ được dùng để Tìm kiếm và hiển thị trên DataGridView |
| Nút Thêm | Khi Click vào thì các giá trị đã nhập sẽ được dùng để thêm mới vào bảng ChitietHOADON |
| Nút Sửa | Khi Click vào thì các giá trị đã nhập sẽ được dùng để cập nhật vào bảng ChitietHOADON. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Xóa | Khi Click vào thì bản ghi có Mã Hóa đơn + Mã Hàng được nhập sẽ bị xóa trong bảng ChitietHOADON. Chức năng bị vô hiệu hóa đối với tài khoản User |
| Nút Refresh | Khi Click vào thì form sẽ được load lại nếu trước đó sử dụng nút Tìm Kiếm |
| Các Nút truy cập Bảng khác | Khi Click vào thì sẽ mở các form khác và ẩn form hiện tại |

# Giải quyết vấn đề dữ liệu lớn

Giả sử lượng dữ liệu rất lớn, không đủ lưu trong một ổ đĩa.

🢡Phương án: Tạo Database trên Cloud – Microsoft Azure *(Chưa thực hiện được)*

Thay vì tạo dữ liệu trên máy thì sẽ tạo dữ liệu online trên AZURE

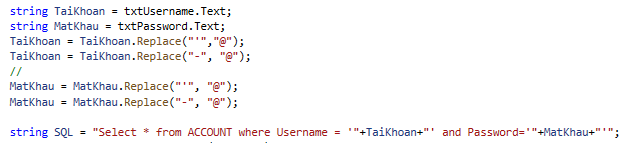
Azure SQL Database là dịch vụ cơ sở dữ liệu đám mây thông minh, có thể mở rộng, cung cấp khả năng tương thích động cơ SQL Server rộng nhất.Cơ sở dữ liệu SQL Azure được xây dựng trên Microsoft SQL Server. Cho qui mô lớn, công nghệ này cung cấp môi trường SQL Server trong đám mây, bổ sung với Index, View, Store Procedure, Trigger,…. Dữ liệu này có thể được truy xuất bằng ADO.Net và các giao tiếp truy xuất dữ liệu Windows khác.

Ở AZURE có nhiều cấu hình SQL Database. Tùy theo giá tiền chi trả, sự lựa chọn  Database sẽ có tốc độ truy cập khác nhau

# Phòng chống SQL Injection

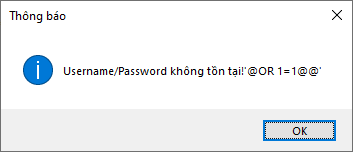
**SQL Injection** là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác delete, insert, update, v.v. trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy. SQL Injection thường được biết đến như là một [vật trung gian](https://vi.wikipedia.org/w/index.php?title=V%E1%BA%ADt_trung_gian_(m%C3%A3_%C4%91%E1%BB%99c)&action=edit&redlink=1) tấn công trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như [SQL Server](https://vi.wikipedia.org/w/index.php?title=SQL_Server&action=edit&redlink=1), [MySQL](https://vi.wikipedia.org/wiki/MySQL), [Oracle](https://vi.wikipedia.org/wiki/Oracle), [DB2](https://vi.wikipedia.org/wiki/DB2), [Sysbase](https://vi.wikipedia.org/w/index.php?title=Sysbase&action=edit&redlink=1)...

+ *Lỗi không kiểm tra ký tự thoát truy vấn*: Đây là dạng lỗi SQL injection xảy ra khi thiếu đoạn mã kiểm tra dữ liệu đầu vào trong câu truy vấn SQL

Cách xử lý đơn giản: Thay thế các ký tự đặc biệt thành các ký tự có thể đọc được

Hình 9.1 Thay thế các ký tự đặc biệt

Thử nhập chuỗi ‘OR 1=1-- vào TextBox Username, Password của form Đăng nhập và kiểm tra bằng MessageBox



Hình 9.2 Kiểm tra 'OR 1=1--