An toàn và toàn vẹn dữ liệu

Đặt vấn đề

- Mục đích của CSDL
  - Lưu trữ lâu dài
  - Khai thác hiệu quả
- Yêu cầu đ/v CSDL
  - Đảm bảo tính toàn vẹn đ/v CSDL
    - Tránh sai sót khi tạo lập và cập nhật CSDL ⇨ định nghĩa và kiểm tra các ràng buộc DL
    - Tránh sai sót trong quá trình thao tác cập nhật với CSDL ⇨ kiểm tra tính toàn vẹn đ/v các thao tác cập nhật, đặc biệt đ/v các thao tác cập nhật đồng thời từ nhiều người sử dụng
  - Đảm bảo tính an toàn đ/v CSDL
    - Tránh truy nhập DL không hợp lệ từ phía người dùng ⇨ phân quyền và kiểm tra quyền hạn người sử dụng

Nội dung

- An toàn dữ liệu
  - Xác minh người sử dụng
  - Kiểm tra quyền truy nhập của người sử dụng
  - Các câu lệnh an toàn dữ liệu trong SQL
- Toàn vẹn dữ liệu
  - Các ràng buộc toàn vẹn trong SQL
  - Quản trị giao dịch và điều khiển tương tranh

An toàn dữ liệu

- **Định nghĩa:** *Tính an toàn dữ liệu là sự bảo vệ dữ liệu trong cơ sở dữ liệu chống lại những truy nhập, sửa đổi hay phá hủy bất hợp pháp.*
  - *Người sử dụng hợp pháp phải cần được cấp phép hay ủy quyền.*
  - *Những nhóm người dùng khác nhau trong hệ CSDL có quyền sử dụng khác nhau.*

An toàn dữ liệu

- Cần các cơ chế *quản lý người dùng* cho phép
  - Xác minh người dùng
  - Kiểm tra quyền hạn của người dùng:
    - Xác định khung nhìn của người dùng
    - Xác định các thao tác hợp lệ với từng (nhóm) người dùng trên khung nhìn

5

Các quyền truy nhập của người sử dụng

- Quyền đọc dữ liệu: được phép đọc một phần hay toàn bộ dữ liệu trong CSDL
- Quyền cập nhật dữ liệu: được phép sửa đổi một số giá trị nhưng không được xóa dữ liệu trong CSDL
- Quyền xóa dữ liệu: được phép xóa dữ liệu trong CSDL
- Quyền bổ sung dữ liệu: được phép thêm dữ liệu mới vào trong CSDL nhưng không được phép thay đổi dữ liệu
- Quyền tạo chỉ dẫn trên các quan hệ trong CSDL
- Quyền thay đổi sơ đồ cơ sở dữ liệu: thêm hay xóa các thuộc tính của các quan hệ trong CSDL
- Quyền loại bỏ quan hệ trong CSDL
- Quyền quản lý tài nguyên: được phép thêm các quan hệ mới vào CSDL

6

Trách nhiệm của người quản trị hệ thống

- Cung cấp một phương tiện cho người sử dụng để hệ thống có thể nhận biết được người sử dụng →Xác minh người sử dụng
- Xác định các quyền cụ thể cho mỗi người sử dụng hay một nhóm người sử dụng → Phân quyền người sử dụng

7

Xác minh người dùng

- Sử dụng tài khoản của người dùng
  - Tên truy nhập
  - Mật khẩu
- Sử dụng hàm kiểm tra F(x)
  - Cho 1 giá trị ngẫu nhiên x
  - Người dùng phải biết hàm F để tính giá trị của nó
- Sử dụng thẻ điện tử, thẻ thông minh
- Sử dụng nhận dạng tiếng nói, vân tay, ...

8

Kiểm tra quyền của người dùng

Mục đích: Xác định quyền hạn của (nhóm) người dùng

- Xác định các khung nhìn để hạn chế truy nhập đến một phần của CSDL
- Xác định và kiểm soát các thao tác trên các khung nhìn

9

Phân quyền người dùng

- Đ/v người khai thác CSDL
  - Quyền đọc dữ liệu
  - Quyền sửa đổi dữ liệu
  - Quyền bổ sung dữ liệu
  - Quyền xoá dữ liệu
  - ...
- Đ/v người quản trị CSDL
  - Quyền tạo chỉ dẫn
  - Quyền quản lý tài nguyên: thêm/xoá các quan hệ
  - Quyền thay đổi cấu trúc DL: thêm/sửa/xoá các thuộc tính của các quan hệ
  - ...
- ...

10

Các câu lệnh an toàn dữ liệu trong SQL

- Câu lệnh tạo người dùng
- Câu lệnh tạo khung nhìn
- Câu lệnh phân quyền cho người sử dụng:
  - Trao quyền
  - Thu hồi quyền

11

Lệnh tạo (nhóm) người dùng

- Cú pháp
  - Tạo người dùng

    CREATE USER *username*
    IDENTIFIED {BY *password* | EXTERNALLY | GLOBALLY AS '*external_name*'};

  - Xoá người dùng

    DROP USER name [CASCADE];

- Ví dụ

  CREATE USER *tin123K47*
  IDENTIFIED BY nmcsdl

12

Lệnh tạo khung nhìn

- CREATE VIEW <view name> [(column list)] AS <SQL query>

13

Lệnh phân quyền cho người dùng

- Trao quyền:

  Grant <Privilege> On <Object> To <user>
  [With Grant Option]

- Thu hồi quyền:

  REVOKE <Privilege> ON <Object> FROM <user>
  [RESTRICT | CASCADE]

Privilege = {Insert | Update | Delete | Select |
Create Alter | Drop | Read | Write}
Object = {Table | View}

14

Ví dụ câu lệnh tạo khung nhìn

Cho cơ sở dữ liệu gồm 2 quan hệ:
Nhânviên(Id,Họtên,ĐC,Lương,NămBD,Đánhgiá,PhòngCT)
Phòng(PId, Tên, ĐC, Điệnthoại, Trưởngphòng)

- Câu lệnh tạo khung nhìn cho một nhân viên của phòng Khoa Học có thể được định nghĩa như sau:

```
CREATE VIEW NVKH(HọtênNhânviên, Địachỉliênlạc) AS
SELECT Họtên,Địachỉ FROM Nhânviên
WHERE PhòngCT IN
    (SELECT PId FROM Phòng WHERE Tên ='Khoa Học')
```

15

Ví dụ câu lệnh phân quyền cho NSD

- Trao quyền đọc, ghi, tìm kiếm, sửa đổi dữ liệu cho nhân viên tên Hoa của phòng Khoa học trên khung nhìn vừa tạo lập trong phần trước

  GRANT read, write, select, update ON NVKH TO Hoa;

- Trao quyền cho trưởng phòng Khoa học – ông HungNC

  GRANT read, write, select, update, delete ON NVKH TO HungNC WITH GRANT OPTION;

16

Câu lệnh thu hồi quyền của NSD (tiếp)

- Thu hồi quyền của trưởng phòng Khoa học – chỉ thu hồi quyền của ông HungNC

REVOKE update,delete ON NVKH FROM HungNC RESTRICT

17

Toàn vẹn dữ liệu

- Mục đích: đảm bảo tính đúng đắn của DL trong quá trình thao tác cập nhật (thêm, sửa, xoá DL)
- Yêu cầu
  - Khai báo và kiểm tra các ràng buộc toàn vẹn DL khi thực hiện các thao tác thêm, sửa, xoá
  - Sử dụng các triggers
  - Kiểm tra tính đúng đắn của các thao tác cập nhật đồng thời trên CSDL
    - Quản trị giao dịch
    - Điều khiển tương tranh

18

Các ràng buộc toàn vẹn

- Mục đích: định nghĩa các quy tắc, các điều kiện đối với toàn bộ DL trong CSDL
- Phân loại ràng buộc:
  - Ràng buộc về miền giá trị
    - Trên 1 thuộc tính
    - Trên nhiều thuộc tính (cùng 1 bộ)
    - Trên nhiều bộ
  - Ràng buộc về khoá
    - Trên 1 quan hệ: khoá chính
    - Trên nhiều quan hệ: khoá ngoài

19

Lệnh đ/n ràng buộc miền giá trị

- Cú pháp

  CONSTRAINT <ten-rang-buoc> CHECK <dieu-kien>
- Ví dụ:
  - Trong bảng Nhânviên

  CONSTRAINT gtLuong CHECK ((Luong>=0) and (Luong <=1000000))

20

Lệnh đ/n ràng buộc khoá chính

- Cú pháp
  CONSTRAINT <ten-rang-buoc>
  PRIMARY KEY <cac-cot-khoa>
- Ví dụ
  – Trong bảng Nhânviên
  CONSTRAINT NV-Kchinh
  PRIMARY KEY Id
  – Trong bảng Phòng
  CONSTRAINT Phòng-Kchinh
  PRIMARY KEY PId

21

Lệnh đ/n ràng buộc khoá ngoài

- Cú pháp
  CONSTRAINT <ten-rang-buoc>
  FOREIGN KEY <cac-cot-khoa>
  REFERENCES <ten-bang>[khoa-tham-chieu]
- Ví dụ: Trong bảng Nhânviên
  CONSTRAINT Phong-NV FOREIGN KEY PhongCT
  REFERENCES Phong[PId]

22

Trigger

- Đ/n
  – Là các xử lý được gắn với các bảng DL
  – Được tự động kích hoạt khi thực hiện các thao tác thêm, sửa, xoá bản ghi
- Cú pháp
  CREATE [OR REPLACE] TRIGGER *<trigger_name>*
  {BEFORE | AFTER | INSTEAD OF }
  {UPDATE | INSERT | DELETE}
  [OF <attribute_name>] ON <table name>
  [FOR EACH ROW]
  BEGIN
  << trigger body goes here >>
  END *<trigger_name>;*

23

Ví dụ

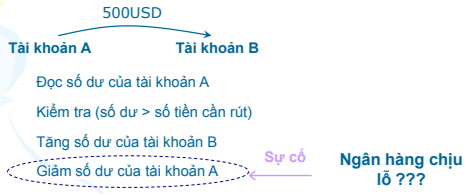
Cho cơ sở dữ liệu gồm 2 quan hệ:
Nhânviên(Id,Họtên,ĐC,Lương,NămBD,Đánhgiá,PhòngCT)
Phòng(PId, Tên, ĐC, Điệnthoại, Trưởngphòng)

- **Xóa Phòng lan truyền**
  CREATE TRIGGER
  DELETE ON Phòng
  DELETE FROM Nhânviên WHERE PhongCT = old.PId ;
- Một nhân viên bao giờ cũng có lương ít hơn lương người trưởng phòng, điều kiện này phải được kiểm tra khi thêm bộ dữ liệu.

```
CREATE TRIGGER ThemNV INSERT ON Nhânviên
IF new.Lương > (SELECT E.Lương FROM Phòng, Nhânviên AS E WHERE
    E.Id = Trưởngphòng AND IF new.PhongCT = PId)
THEN ABORT;
```

24

Giao dịch – ví dụ

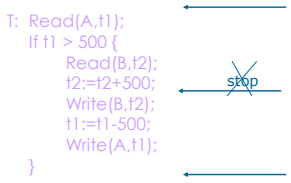


Giao dịch

- Đ/n: một tập các thao tác được xử lý như một đơn vị không chia cắt được
  - Cho phép đảm bảo tính nhất quán và tính đúng đắn của dữ liệu
- Tính chất ACID
  - Nguyên tố (***A**tomicity*) } Điều khiển tương tranh
  - Tính nhất quán (***C**onsistency*)
  - Tính cô lập (***I**solation*) } Phục hồi dữ liệu
  - Tính bền vững (***D**urability*)

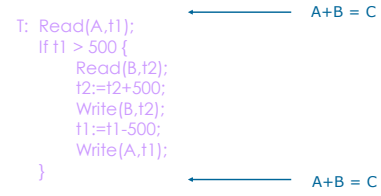
Tính nguyên tố

- Đ/n: Hoặc là toàn bộ hành động của giao dịch được thực hiện hoặc không có hành động nào được thực hiện
- Ví dụ:



Tính nhất quán

- Đ/n: Tính nhất quán của dữ liệu trước khi bắt đầu và sau khi kết thúc giao dịch
- Ví dụ



Tính cô lập

- Đ/n: 1 giao dịch được tiến hành độc lập với các giao dịch khác tiến hành đồng thời
- Ví dụ: A= 5000, B= 3000

```
T:  Read(A,t1);
    If t1 > 500 {
        Read(B,t2);
        t2:=t2+500;
        Write(B,t2);
        t1:=t1-500;
        Write(A,t1);
    }
```

← T': A+B (= 5000+3500)

← (A+B = 4500+3500)

29

Tính bền vững

- Đ/n
  - Mọi thay đổi mà giao dịch thực hiện trên CSDL phải được ghi nhận bền vững
- Ví dụ: A= 5000, B= 3000

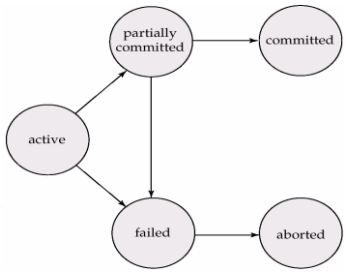
```
T:  Read(A,t1);
    If t1 > 500 {
        Read(B,t2);
        t2:=t2+500;
        Write(B,t2);
        t1:=t1-500;
        Write(A,t1);
    }
```

← Sự cố

A= 4500, B=3500

30

Trạng thái của giao dịch



31

Giao diện cho giao dịch

- Giao diện chính
  - Begin Trans
  - Commit ()
  - Abort()
- Điểm ghi nhớ (save point)
  - Savepoint Save()
  - Rollback (savepoint) // savepoint = 0 ==> Abort

32

Điều khiển tương tranh

- Mục đích: tránh sự đụng độ giữa các giao dịch (một dãy các thao tác) trên cùng một đối tượng có thể làm mất tính nhất quán của DL

T0:	T1:

read(A);
A := A -50;
write(A);
read(B);
B := B + 50;
write(B);
	read(A);
	temp := A *0.1;
	A := A -temp;
	write(A);
	read(B);
	B := B + temp;
	write(B);

Ví dụ về lịch thực hiện

T0	T1
read(A)	
A := A - 50	
write(A)	
read(B)	
B := B + 50	
write(B)	
	read(A)
	temp := A * 0.1
	A := A -temp
	write(A)
	read(B)
	B := B + temp
	write(B)

T0	T1
	read(A)
	temp := A * 0.1
	A := A -temp
	write(A)
	read(B)
	B := B + temp
	write(B)
read(A)	
A := A - 50	
write(A)	
read(B)	
B := B + 50	
write(B)	

Kỹ thuật khoá

- Mục đích
  - Đảm bảo việc truy nhập đến các DL được thực hiện theo phương pháp loại trừ nhau
- Các kiểu khoá
  - Chia sẻ: có thể đọc nhưng không ghi DL
  - Độc quyền: đọc và ghi DL
- Ký hiệu
  - LS(D): khoá chia sẻ
  - LX(D): khoá độc quyền
  - UN(D): mở khoá
- Tính tương thích

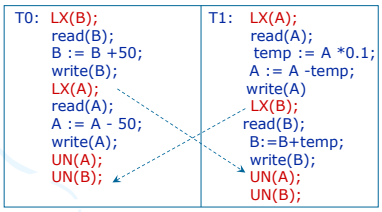
	LS	LX
LS	true	false
LX	false	false

Ví dụ

T0:	T1:

LX(A);
read(A);
A := A -50;
write(A);
LX(B);
read(B);
B := B + 50;
write(B);
UN(A);
UN(B);
	LX(A);
	read(A);
	temp := A *0.1;
	A := A -temp;
	write(A)
	LX(B);
	read(B);
	B:=B+temp;
	write(B);
	UN(A);
	UN(B);

Khoá chết *(deadlock)*



37

Kỹ thuật gán nhãn

- Mục đích:
  - Điều khiển việc truy nhập DL dựa trên nhãn thời gian
- Gán nhãn cho giao dịch T: timestamp(T)
- Gán nhãn cho các thao tác của giao dịch
- Nguyên tắc điều khiển truy nhập:
  - Một giao dịch được phép thực hiện một thao tác trên X nếu cập nhật cuối cùng trên X được thực hiện bởi một giao dịch già hơn (có nhãn nhỏ hơn).

38

Các vấn đề về quản trị giao dịch

- Các kỹ thuật điều khiển tương tranh
  - các chế độ khoá, giải quyết khoá chết
  - kỹ thuật gán nhãn
- Lập lịch
- Các kỹ thuật phục hồi (*recovery*)
- ...

39

Kết luận

Để đảm bảo tính an toàn và toàn vẹn dữ liệu

- Đ/v người thiết kế CSDL
  - Phải định nghĩa các ràng buộc toàn vẹn về dữ liệu
- Đ/v người quản trị hệ thống
  - Phải định nghĩa các khung nhìn
  - Phải phân quyền cho (nhóm) người dùng
- Đ/v hệ CSDL
  - Phải xác minh được người dùng
  - Phải kiểm tra các ràng buộc DL một cách tự động
  - Phải đảm bảo các tính chất ACID cho giao dịch người dùng

40