PROTECȚIA DATELOR ȘI CONTROLUL ACCESULUI ÎN SGBD

MALACHI Vitalie

Universitatea Tehnică a Moldovei

Abstract: *În acest articol sunt descrise unele aspecte ale protecţiei bazelor de date în scopul asigurării securităţii informaţiilor valoroase stocate în baza de date a unui sistem informatic, fiind considerate teme de maximă actualitate şi de maximă importanţă pentru securitatea datelor.*

Cuvinte cheie: *SGBD, securitate, integritate, protecţia datelor.*

1. Introducere

Dezvoltarea sistemelor de baze de date reprezintă un aspect important în domeniul tehnologiei informaţiei, având un impact decisiv asupra modului de organizare şi funcţionare a numeroaselor instituţii şi servicii.

Obiectivul general al unui sistem de gestiune a bazelor de date (SGBD) este de a furniza suportul software complet pentru dezvoltarea de aplicaţii informatice cu baze de date. Alte obiective ale SGBD sunt:

- Asigurarea independenţei datelor. O bază de date este realizată pentru o gamă largă de utilizatori, care au la dispoziţie un volum mare de date. SGBD-ul trebuie să-i permită la un moment dat unui utilizator să "vadă" (să-şi construiască o viziune) doar o parte din baza de date şi anume numai acele date care îl interesează. Administratorul bazei de date trebuie să aibă libertatea de a schimba structura de memorare sau strategia de acces, ca răspuns la cerinţele noi apărute, fără a modifica aplicaţiile existente (sistem deschis).
- Redundanţă minimă şi controlată a datelor. Spre deosebire de sistemele clasice (cu fişiere) de prelucrare automată a datelor, stocarea informaţiilor în bazele de date se face astfel încât datele să nu fie multiplicate. Exemplul tipic de redundanţă controlată acceptată este cea apărută la proiectare bazelor de date relaţionale prin tehnica de normalizare.
- Asigurarea facilităţii de utilizare a datelor. Aceasta presupune că SGBD-ul să aibă nişte componente specializate pentru diferite operaţii de utilizare: folosirea datelor de către mai mulţi utilizatori în diferite scopuri; accesul cât mai simplu al utilizatorilor la date, fără ca ei să fie nevoiţi să cunoască structura întregii baze de date; existenţa unor limbaje performante de regăsire a datelor care permit exprimarea interactivă a unor cereri de regăsire a datelor şi indicarea unor reguli pentru editarea informaţiilor solicitate.
- Protecţia datelor. Această sarcină a SGBD este foarte actuală în condiţiile fraudelor cibernetice de amploare tot mai frecvente din zilele noastre. În sistemele de bază de date, protecţia datelor se asigură sub două aspecte: securitatea şi integritatea datelor.
- Performanţele globale. Performanţele globale ale aplicaţiei sunt influenţate de SGBD. Acesta trebuie să gestioneze un volum mare de date de o complexitate ridicată, într-un anumit timp de acces rezonabil pentru diferiţi utilizatori. Pentru toate aceste lucruri SGBD-ul foloseşte diferite metode de acces, tehnici de optimizare, tipuri de date. Implementarea lor se face în componente specializate ale SGBD-ului.

2. Protecţia datelor în SGBD

Securitatea (confidenţialitatea) datelor semnifică faptul că accesul la date se face numai printr-o autorizare corespunzătoare şi doar controlat (sarcina administratorului bazei de date cu ajutorul SGBD-ului). În acest sens, SGBD-ul permite:

- Autorizarea şi controlul accesului la date. Este realizat de SGBD prin intermediul parolelor;
- Utilizarea viziunilor (view). Este asigurată de SGBD pentru reprezentarea schemelor externe ale bazei de date;
- Realizarea unor proceduri speciale de acces asupra datelor este permisă de SGBD.
- Criptarea datelor. Este asigurată de SGBD prin oferirea unor rutine de criptare (codificare) a datelor apelate automat sau la cerere şi prin existenţa unor instrumente care permit

utilizatorului să realizeze propriile rutine de criptare. Criptarea şi decriptarea se realizează după algoritmi specifici, cu o cheie (parolă) de acces la rutină.

Componentele unui sistem de criptare sunt:

- Algoritmul de criptare, care transformă datele iniţiale într-o formă cifrată (codificată);
- Cheia de criptare ,care permite intrarea în algoritmul de criptare;
- Algoritmul de decriptare , care transformă datele din forma criptată în cea iniţială;
- Cheia de decriptare, de intrare în algoritmul de decriptare.

Integritatea datelor este asigurată de către componentele SGBD-ului tratând separat cauzele care pot altera baza de date: integritatea semantică, controlul accesului concurent, salvarea/restaurarea.

Integritatea semantică este asigurată prin operaţii efectuate de SGBD asupra datelor şi a prelucrărilor.

Accesul concurent asigură coerenţa datelor şi este un obiectiv al SGBD-ului care este foarte actual mai ales la baze de date distribuite. În acest sens SGBD-ul are o unitate distinctă de prelucrare a datelor numită tranzacţie, care este constituită dintr-o secvenţă de operaţii marcată de puncte de început şi sfârşit.

La execuţia concurentă a tranzacţiilor SGBD-ul trebuie să asigure blocarea datelor utilizate la un moment dat. Aceasta înseamnă că se interzice accesul celorlalte tranzacţii concurente la aceleaşi date, până se termină tranzacţia curentă.

Sub aspectul accesului concurent putem vorbi si despre partajabilitatea datelor, care se referă atât la asigurarea accesului mai multor utilizatori la aceleaşi date, cât şi la posibilitatea dezvoltării unor aplicaţii fără a se modifica structura bazei de date. Problema partajabilităţii se pune la un nivel superior pentru SGBD-urile care permit lucrul în reţea.

Interblocarea este situaţia în care două tranzacţii blochează anumite resurse, apoi solicită fiecare resursele blocate de cealaltă. La nivelul de SGBD trebuie să existe facilitatea de prevenire sau rezolvare a interblocării.

Prevenirea interblocării presupune că programele blochează toate resursele de care au nevoie încă de la începutul fiecărei tranzacţii (greu de precizat).

Soluţionarea interblocării presupune că există nişte mecanisme pentru detectarea şi eliminarea interblocării (de exemplu graful dependenţelor proceselor de executat).

Salvarea/restaurarea (backup/recovery) ca facilitate a SGBD-ului permite refacerea consistenţei datelor care au fost alterate fizic din diferite motive.

Salvarea datelor este un proces de stocare prin realizarea de copii de siguranţă şi prin jurnalizarea tranzacţiilor şi a imaginilor. SGBD-ul poate asigura salvarea automat sau la cererea administratorului bazei de date.

Restaurarea porneşte de la colecţii de date stocate prin salvare şi reface consistenţa bazei de date, minimizând prelucrările pierdute. Restaurarea este asigurată automat de SGBD, dar se poate realiza şi manual.

Concluzii

Protecţia datelor şi controlul accesului în SGBD este un domeniu mult prea vast şi cu prea multe domenii conexe pentru a fi descris complet undeva. Lumea este în continua mişcare, cerinţele de securitate si confidenţialitate cresc pe zi ce trece, ameninţările ţin pasul. Asigurarea securităţii bazei de date trebuie să se facă din exterior în interior, aceasta implicând asigurarea securităţii pornind de la nivelul fizic şi terminând cu nivelul de date (fizic,de reţea, gazdă, aplicaţii şi date).

Bibliografie

1. DATE, C.J., An Introduction to Database Systems (8th Edition), Addison-Wesley, 2004, cap 13.
2. RAMAKRISHNAN, R., Database Management Systems. McGraw-Hill, 2007, cap. 17, http://pages.cs.wisc.edu/~dbbook/openAccess/thirdEdition/slides/slides3ed.html
4. How to Enter SQL Comments, http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.sqls.doc/sqls 36.htm