(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 127921 A0**
(51) Int.Cl.
G06F 17/30 (2006.01);
G06Q 10/00 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2011 01395**

(22) Data de depozit: **14.12.2011**

(41) Data publicării cererii:
30.10.2012 BOPI nr. **10/2012**

(71) Solicitant:
• **TEAMNET INTERNATIONAL SA**,
SPLAIUL INDEPENDENŢEI NR. 319, SEMA PARC, CITY BUILDING 1, ET. 8, SECTOR 6, BUCUREŞTI, B, RO

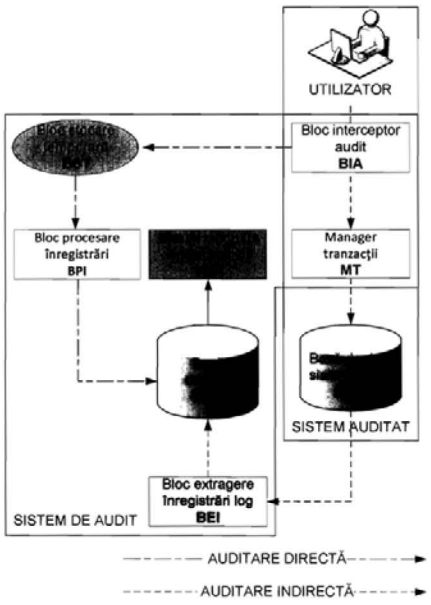
(72) Inventatori:
• **STAN GEORGE-MIHAIL**, *STR. GLĂDIŢEI NR. 42, BL. T7, ET. 9, AP. 904, SECTOR 4, BUCUREŞTI, B, RO;*
• **NEDELCU RADU-BOGDAN**,
STR. LOCOTENENT GHEORGHE SAIDAC NR. 4, BL. 35, SC. D, AP. 64, SECTOR 6, BUCUREŞTI, B, RO;
• **TRAŞCU ION-OVIDIU**,
STR. MARINARILOR NR. 12-16, BL. IX/1, SC. A, ET. 1, AP. 5, SECTOR 1, BUCUREŞTI, B, RO

(54) # METODĂ ŞI SISTEM DE AUDITARE A MODIFICĂRILOR EFECTUATE ASUPRA DATELOR

(57) **Rezumat:**

Invenţia se referă la o metodă şi la un sistem de audit al operaţiilor efectuate asupra înregistrărilor dintr-o bază de date. Metoda se bazează pe urmărirea schimbărilor efectuate de un operator pe trei niveluri: nivelul interfaţă grafică, nivelul logică de aplicaţii şi nivelul bază de date. Metoda foloseşte fişierele de tranzacţii ale bazei de date, pentru a identifica schimbările aduse datelor, gestionează corespondenţa între ecrane, operaţiile de logică de business şi datele modificate. Sistemul de audit oferă o imagine completă a interacţiunii utilizator-sistem şi permite elaborarea unor rapoarte care determină toate modificările operate în baza de date de către utilizator într-un interval de timp, sub forma unor date existente înainte de tranzacţie şi date modificate după tranzacţie. Sistemul de audit înregistrează adresa de la care s-au efectuat operaţiile, data, ora, precum şi alte date utile identificării utilizatorului. Sistemul de audit funcţionează în tandem cu un sistem de securitate, şi permite executarea unor operaţii asupra datelor sau asupra nivelului de business al aplicaţiei numai dacă accesul a fost validat de către sistemul de securitate.

Revendicări: 2
Figuri: 1



RO 127921 A0

DESCRIERE TEHNICĂ

Invenţia prezentată se referă la o metodă şi la un sistem, realizat pe baza metodei, pentru auditarea operaţiilor efectuate de către utilizatorii unui sistem informatic într-o bază de date.

Utilitatea sistemului de auditare provine din nevoia de a asigura un nivel înalt de trasabilitate între acţiunile utilizatorilor unui sistem informatic şi modul în care aceste acţiuni modifică starea datelor sistemului. Sistemele de audit sunt impuse atât de respectarea standardelor de securitate informatică în majoritatea aplicaţiilor în care utilizatorii joacă rolul central, cât şi pentru implementarea cerinţelor specifice proprietarilor sistemelor informatice.

De-a lungul timpului, au fost create diverse sisteme de audit, majoritatea bazându-se pe intercepţia operaţiilor executate la nivel de business. Această metodă prezintă însă dezavantajul că orice modificare executată asupra bazei de date, fără a folosi aplicaţia (de exemplu printr-un client de management specific bazei de date), nu va fi auditată de către sistemul de audit pentru că acesta acţionează exclusiv la nivel de business, un nivel superior celui de bază de date.

A doua metodă de audit cunoscută efectuează auditul la nivel de bază de date, folosind mecanisme care există în majoritatea bazelor de date, denumite generic „triggers". Acest mecanism presupune că baza de date, înainte de modificarea oricărei tabele, apelează subrutine definite de programatori. Această metodă prezintă însa dezavantaje majore care afectează performanţa sistemului auditat astfel:

- apelul mecanismului „trigger" este un apel sincron, care reduce performanţele sistemului auditat în cazul aplicaţiilor care folosesc în mod intensiv baza de date pentru operaţii de creare, modificare sau ştergere înregistrări;
- modificarea structurii bazei de date auditate presupune şi modificarea sistemului de audit, având în vedere că sunt necesare rutine pentru fiecare tabelă auditată.

A treia categorie de sisteme de audit se bazează pe interceptarea mesajelor de modificare a stării bazelor de date, numite generic operaţii CRUD (Create Update Delete). Acest mecanism, deşi generic, este greu de implementat datorită faptului că

trebuie să ruleze continuu pentru a intercepta modificările şi prezintă inconvenientul că stochează numai valorile noi, neavând acces la valorile vechi ale datelor.

Metoda care face obiectul invenţiei se referă la auditarea unui sistem informatic care are în compunere o bază de date şi presupune parcurgerea a două etape:

- Etapa 1. Interceptarea în timp real a operaţiilor efectuate de utilizator la nivel de interfaţă şi la nivel de operaţii de business (auditarea directă);
- Etapa 2. Colectarea ulterioară a înregistrărilor despre modificările efectuate în baza de date (auditarea indirectă).

Etapa 1 presupune interceptarea oricărui apel de funcţie dinspre interfaţa utilizator către logica de business şi marcarea acestuia cu un identificator de tranzacţie. Identificatorul de tranzacţie asigură vizualizarea caracteristicilor conectării fiecărui utilizator la baza de date, prin înregistrarea următoarelor informaţii:

- numele staţiei de lucru a utilizatorului;
- momentul conectării şi deconectării utilizatorului;
- operaţiile efectuate de utilizator în cadrul sesiunii;
- detaliile operaţiei, respectiv vizualizarea datelor anterior şi după execuţia operaţiei din baza de date.

Asupra acestor înregistrări se pot aplica operaţiuni de filtrare pentru a determina cu precizie autorul, operaţiile executate şi impactul asupra sistemului auditat. În urma filtrării se pot afişa următoarele tipuri de operaţii:

- operaţiile efectuate pe parcursul sesiunii de lucru a unui utilizator;
- operaţiile efectuate de un anumit utilizator;
- operaţiile efectuate de la o anumită staţie de lucru;
- operaţiile efectuate pe toate tabelele din baza de date precum şi datele modificate de acesta (prin memorarea datelor înainte şi dupa operaţia respectivă);
- operaţiile efectuate pe anumite entităţi de business.

Etapa 2 presupune, conform metodei, marcarea oricărui apel de funcţie dinspre interfaţa utilizator către logica de business cu identificatorul specific de tranzacţie, care se memorează în log-ul tranzacţional al bazei de date. Citirea acestui indicator permite obţinerea următoarelor informaţii:

- activitatea declanşatoare;

- activităţile de business apelate;
- efectele din baza de date.

Sistemul pentru aplicarea metodei de auditare a modificărilor efectuate asupra datelor, este compus, conform figurii, dintr-un bloc interceptor de audit **BIA**, integrat în sistemul informatic auditat. Blocul interceptor de audit **BIA** are rolul de a intercepta operaţiile efectuate de către utilizator atât asupra interfeţei cât şi asupra sistemului de bussines, fără a afecta perfomanţa aplicaţiei auditate, precum şi de a marca informaţiile auditate cu un identificator unic care va fi transmis blocului manager de tranzacţii **MT**. Blocul interceptor de audit **BIA** este complet integrat din punct de vedere tehnologic în mecanismul de gestiune a operaţiilor efectuate de către utilizatori, pentru a avea acces în mod nativ la datele despre operaţia efectuată, fără a efectua operaţii suplimentare asupra contextului de procesare a operaţiei şi astfel nu are impact asupra performanţei sistemului auditat. De asemenea, acest bloc dispune de capabilitatea de a genera un identificator unic al fiecărei operaţii şi poate astfel să auditeze şi sisteme distribuite atât din punct de vedere hardware cât şi geografic.

Blocul interceptor de audit **BIA** este conectat cu blocul de stocare temporară **BST** căruia îi transmite datele pentru interceptarea în timp real a operaţiilor efectuate de utilizator (auditarea directă) şi cu blocul manager de tranzacţii **MT** pentru colectarea ulterioară a modificărilor efectuate asupra bazei de date (auditarea indirectă).

Calea care implementează etapa de auditare directă este compusă din blocul de stocare temporară **BST** şi blocul de procesare înregistrări **BPI**.

Blocul de stocare temporară **BST** este un bloc optimizat pentru scrieri asincrone, repetate şi la intervale de timp foarte scurte. Blocul de stocare temporară **BST** are şi capabilitatea de a permite accesul securizat atât pentru operaţiile de scriere cât şi pentru cele de citire a datelor.

Blocul de procesare înregistrări **BPI** reprezintă componenta specializată în preluarea datelor din blocul de stocare temporară **BST** şi introducerea acestora în baza de date a sistemului de audit **DBB**. Acest sistem este fault-tolerant şi rulează la nivel de sistem de operare pentru a garanta că blocul de stocare temporară **BST** nu va fi supraîncărcat, evitând astfel un blocaj în partea de timp real a sistemului de

audit. Informaţiile aferente etapei de interceptare în timp real sunt apoi depuse de către blocul de procesare înregistrări **BPI** în baza de date a sistemului de audit **DBB**.

Calea care implementează etapa de auditare indirectă este compusă din blocul manager de tranzacţii **MT**, baza de date a sistemului auditat **DBA**, şi blocul de extragere înregistrări log **BEI**.

Blocul manager de tranzacţii **MT** are rolul de a gestiona tranzacţiile efectuate în sistemul auditat, cu scopul de a le marca într-un mod unic ca aparţinând unei anumite sesiuni de lucru a unui anumit utilizator. Pentru marcarea operaţiilor, blocul manager de tranzacţii **MT** foloseşte identificatorul generat şi furnizat de către blocul interceptor de audit **BIA**. Marcarea operaţiilor este necesară pentru blocul de raportare a modificărilor **BRM**, pentru a corela operaţiile business ale utilizatorilor cu modificările efectuate asupra bazei de date, oferind astfel o imagine de ansamblu asupra sistemului auditat.

În cadrul etapei de colectare ulterioară a modificărilor efectuate asupra bazei de date, blocul manager de tranzacţii **MT** marchează următoarele operaţiuni: inserare, modificare şi ştergere. Aceste informaţii sunt stocate în log-ul de tranzacţii şi memorează toate modificările efectuate de utilizatori în baza de date a sistemului auditat **DBA**.

Înregistrările sunt extrase din baza de date a sistemului auditat **DBA** de către blocul de extragere înregistrări log **BEI**, procesate şi stocate în baza de date a sistemului de audit **DBB**. Blocul de extragere înregistrări log **BEI** procesează în mod asincron datele stocate în log-ul bazei de date auditate, **fără a afecta perfomanţele sistemului auditat** sau ale bazei lui de date. Blocul de extragere înregistrări log **BEI** are şi capabilitatea de a extrage înregistrările atât pe baza unui calendar predefinit cât şi la cererea unui administrator de sistem. Informaţiile aferente etapei de colectare ulterioară a modificărilor efectuate asupra bazei de date sunt depuse de către blocul de extragere înregistrări log **BEI** în baza de date a sistemului de audit **DBB**.

Datele referitoare la cele două etape de auditare, stocate în baza de date a sistemului de audit **DBB**, sunt raportate prin intermediul blocului de raportare a modificărilor **BRM**. Blocul de raportare a modificărilor **BRM** are rolul de a corela operaţiile de interfaţă, cele de business şi efectul lor în baza de date prin intermediul identificatorului unic generat de catre blocul interceptor de audit **BIA**. De asemenea,

blocul de raportare a modificărilor **BRM** are capabilităţi extinse de procesare şi furnizare de date agregate pe baza informaţiilor colectate, atât în timp real cât şi în mod asincron şi furnizează rapoarte despre sesiunea deschisă de un utilizator şi despre identitatea utilizatorilor care au efectuat operaţii asupra unei inregistrări specifice în format: date existente înainte de tranzacţie şi date modificate după tranzacţie.

Sistemul de auditare funcţionează în tandem cu sistemul de securitate, şi permite executarea unor operaţii asupra datelor sau asupra nivelului de business al aplicaţiei numai dacă accesul a fost validat de către sistemul de securitate

Revendicări

1. Metodă de auditare a operaţiilor efectuate asupra înregistrărilor dintr-o bază de date **caracterizată prin aceea că** auditarea unui sistem informatic care are în compunere o bază de date are loc, fără a afecta performanţele aplicaţiei auditate, în două etape:

- Etapa 1. Interceptarea în timp real a operaţiilor efectuate de utilizator la nivel de interfaţă şi la nivel de operaţii de business (auditarea directă);
- Etapa 2. Colectarea ulterioară a înregistrărilor despre modificările efectuate în baza de date (auditarea indirectă).

2. Sistem pentru aplicarea metodei de la revendicarea 1, **caracterizat prin aceea că** este alcătuit dintr-un bloc interceptor de audit **BIA**, care are rolul de a intercepta operaţiile efectuate de către utilizator asupra interfeţei cât şi asupra sistemului de bussines şi de a marca informaţiile auditate cu un identificator unic, transmis blocului manager de tranzacţii **MT**. Blocul interceptor de audit **BIA** este conectat cu blocul de stocare temporară **BST** căruia îi transmite datele pentru interceptarea în timp real a operaţiilor efectuate de utilizator (auditarea directă) şi către blocul manager de tranzacţii **MT** pentru colectarea ulterioară a modificărilor efectuate asupra bazei de date (auditarea indirectă).

Calea care implementează etapa de auditare directă este compusă din blocul de stocare temporară **BST** şi blocul de procesare înregistrări **BPI**. Informaţiile aferente etapei de interceptare în timp real sunt depuse de către blocul de procesare înregistrări **BPI** în baza de date a sistemului de audit **DBB**.

Calea care implementează etapa de auditare indirectă este compusă din managerul de tranzacţii **MT**, baza de date a sistemului auditat **DBA**, şi blocul de extragere înregistrări log **BEI**.

Blocul manager de tranzacţii **MT** are rolul de a gestiona tranzacţiile efectuate în sistemul auditat, cu scopul de a le marca într-un mod unic ca aparţinând unei anumite sesiuni de lucru a unui anumit utilizator. Baza de date a sistemului auditat **DBA** stocheaza log-ul de tranzacţii care conţine toate modificările efectuate de către utilizatori asupra acesteia. Înregistrările sunt extrase din baza de date a sistemului auditat **DBA** de către blocul de extragere înregistrări log **BEI**, procesate şi stocate în baza de date a sistemului de audit **DBB**.

Datele referitoare la cele două etape de auditare, stocate în baza de date a sistemului de audit **DBB**, sunt raportate prin intermediul blocului de raportare a modificărilor **BRM**, care are capabilităţi extinse de raportare a operaţiilor executate asupra bazei de date a sistemului informatic auditat.

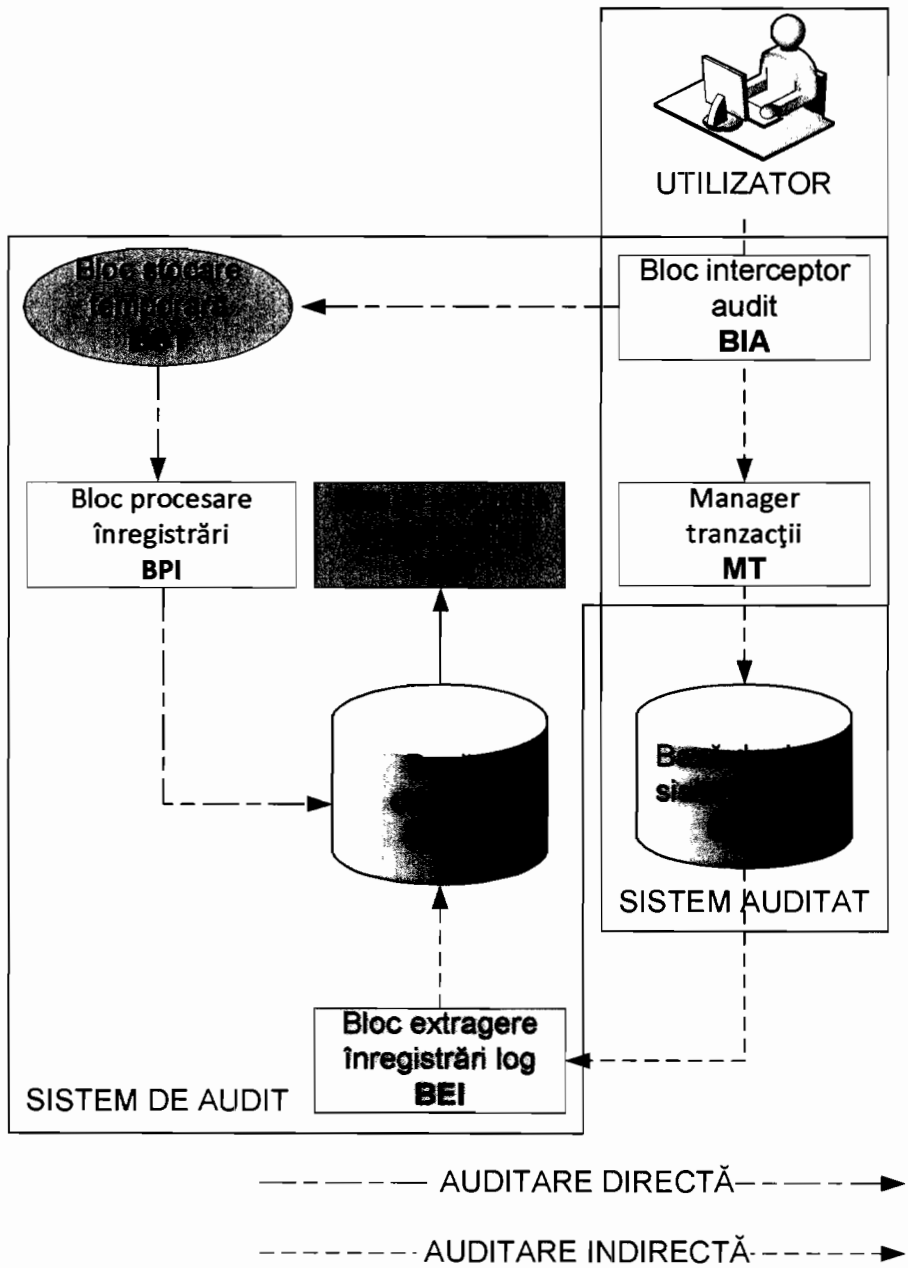

UTILIZATOR
Bloc interceptor audit
BIA
Bloc procesare înregistrări
BPI
Manager tranzacţii
MT
SISTEM AUDITAT
Bloc extragere înregistrări log
BEI
SISTEM DE AUDIT
AUDITARE DIRECTĂ
AUDITARE INDIRECTĂ

Figura 1.