(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 137262 A2**
(51) **Int.Cl.**
G06F 21/64 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2021 00441**

(22) Data de depozit: **29/07/2021**

(41) Data publicării cererii:
30/01/2023 BOPI nr. **1/2023**

(71) Solicitant:
• **UNIVERSITATEA "ALEXANDRU IOAN CUZA" DIN IAŞI**, *BD. CAROL I NR. 11, IAŞI, IS, RO;*
• **AQUASOFT S.R.L.**, *STR.VIRTUŢII, NR.6, SECTOR 6, BUCUREŞTI, B, RO*

(72) Inventatori:
• **STOICA CRISTIAN**, *ŞOS.VIRTUŢII, NR.6, BL.R12, SC.3, ET.3, AP.81, SECTOR 6, BUCUREŞTI, B, RO;*
• **CIOBANU-MOROGAN DIMITRIE-MATEI**, *STR.CIUREA, NR.2-4, BL.P6A+B, SC.C, ET.9, AP.127, SECTOR 2, BUCUREŞTI, B, RO;*
• **ALBOAIE LENUŢA**, *STR.PROF. IOAN PETRU CULIANU NR.58, IAŞI, IS, RO*

Această publicaţie include şi modificările descrierii, revendicărilor şi desenelor depuse conform art. 35 alin. (20) din HG nr. 547/2008

(54) # SISTEM DE PROTECŢIE A DATELOR PRIN CONTROLUL ACCESULUI OPERAŢIILOR DIRECTE DE MODIFICARE A ACESTORA

(57) **Rezumat:**

Invenţia se referă la un sistem de protecţie a datelor prin controlul accesului operaţiilor directe de modificare a acestora. Sistemul de protecţie, conform invenţiei, poate fi implementat ca dispozitiv hardware sau ca program sau rutină software, şi este interpus între un sistem de operare şi un sistem de stocare a datelor, toate operaţiunile executate asupra sistemului de stocare fiind realizate prin intermediul sistemului de protecţie, care previne modificarea sau ştergerea directă a datelor, permiţând doar adăugarea de date noi sau marcarea unor date ca fiind şterse sau înlocuite, dar păstrându-le pe cele anterioare accesibile în istoric.

Revendicări iniţiale: 1
Revendicări amendate: 1
Figuri: 9

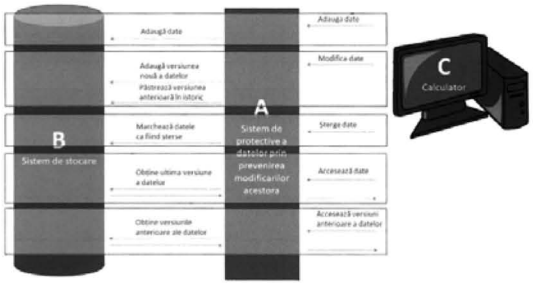

Fig. 9

RO 137262 A2

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2021 00441
Data depozit 29 -07- 2021

RO 137262 A2

27

Sistem de protectie a datelor prin controlul accesului operaţiilor directe de modificare a acestora

Sistem de protectie a datelor prin controlul accesului operaţiilor directe de modificare a acestora.

Acest sistem are scopul de a preveni coruperea sau criptarea datelor de către viruşi sau alte atacuri informatice. Datele stocate pe diverse medii de stocare (discuri, memorii solide) pot fi şterse sau modificate în mod neautorizat ca urmare a unor atacuri asupra calculatorului la care aceste medii sunt conectate. Prin prevenirea oricărei modificări sau ştergeri a datelor stocate, şi prin permiterea exclusivă doar a operaţiilor de adăugare a datelor la cele deja existente, se poate garanta integritatea datelor stocate şi se pot preveni atacuri de tip "ransomeware".

Invenţia se aplică sistemelor de stocare a datelor, prin inserarea unui sistem fizic sau programatic care să prevină ştergerea sau modificarea lor.

Tehnologiile de backup existente (scrierea pe banda a datelor, scrierea pe discuri optice) previn ştergerea sau modificarea datelor. Aceste tehnologii prezintă însă mari dificultăţi de utilizare, pe de o parte, şi nu sunt folosite în timp real, necesitând o copiere periodică a datelor. Această copiere periodică poate lua mult timp, iar datele dintre perioadele de copiere nu sunt protejate până în momentul copierii.

Tehnologia "blockchain" permite stocarea datelor într-un mod care asigură detectarea oricărei modificări a acestora, însă nu previne modificarea propriu-zisă a fişierelor. Sistemul de verificare a integrităţii datelor oferit de tehnologia blockchain nu ajută în momentul în care datele respective sunt şterse sau modificate.

Scopul invenţiei este acela de a asigura integritatea datelor stocate, prin prevenirea modificărilor acestora în urma unor atacuri sau aplicaţii ilicite.

Prin folosirea invenţiei, este posibilă implementarea unei politici de securitate care nu permite ştergerea sau modificarea datelor, ci doar adăugarea acestora la cele deja existente. Astfel, orice modificare care apare este pur şi simplu stocată ca o nouă versiune a datelor precedente. La accesarea datelor, ultima versiune este în mod normal accesată, dar dacă aceasta a fost coruptă, se pot accesa versiunile precedente. Orice atac poate doar sa adauge o versiune coruptă, dar versiunile corecte raman în sistem.

Sistemul este implementat fie într-un dispozitiv hardware, fie ca parte a sistemului de operare, sau ca un driver folosit de sistemul de operare. Sistemul funcţionează în felul următor: atunci când date trebuie scrise pe dispozitivul de stocare protejat de sistem, aceste date sunt trimise sistemului. Sistemul se ocupă cu scrierea datelor pe dispozitivul de stocare, şi nu poate fi evitat. Sistemul adaugă datele pe dispozitivul de stocare, fără a şterge sau modifica datele deja existente. În funcţie de tehnologia folosită, lucrul acesta se poate realiza în mai multe feluri:

SC AQUASoft SRL

Rector,
Prof. Dr. Tudorel Toader

1) Folosind un sistem de fişiere standard

În cazul în care fişierul trimis nu este deja existent în spaţiul de stocare, fişierul este pur şi simplu adăugat (Figura 1).

În cazul în care există deja un fişier cu numele şi poteca fişierului nou, numele fişierului vechi este modificat, în aşa fel încât să poată fi accesat ulterior, şi să fie clară ordinea fişierelor mai vechi. Fişierul nou este scris cu numele actual (Figura 2).

2) Folosind un sistem de control al versiunilor

Sistemul poate implementa un sistem de control al versiunilor (de exemplu tip „git"). În acest caz, dacă datele nu există deja, acestea sunt adăugate (Figura 3).

Dacă datele există deja, o nouă versiune este adăugată (Figura 4).

3) Folosind blocuri şi tehnologie tip blockchain

Datele sunt transformate în unul sau mai multe blocuri care sunt stocate în sistemul de stocare, şi adăugate la blockchain (Figura 5). Astfel, toate versiunile precedente, plus cea nouă, sunt stocate şi accesibile.

Avantajele rezultate din aplicarea invenţiei sunt asigurarea integrităţii datelor, protecţia acestora la modificări ilicite, protecţia acestora la ştergere, protecţia acestora la criptarea ilicită caracteristică atacurilor de tip "ransomware", asigurarea disponibilităţii datelor.

Un exemplu de realizare a invenţiei este prezentat în figura 6. Aici, sistemul de protecţie (A) este conectat la un server (C) care rulează o aplicaţie de comunicaţii de tip Qloud, unde protecţia integrităţii datelor este esenţială, iar sistemul de stocare (B) este conectat la sistemul de protecţie. Sistemul de protecţie foloseşte sistemul PrivateSky, bazat pe un concept numit "brick" (date criptate referentiate prin calcul unei functii de hash asupra conţinutului - content adresable file systems). Pentru stocarea datelor, C trimite o cerere de stocare către A, împreună cu datele care trebuie stocate. A foloseşte funcţiile PrivateSky pentru crearea brick-urilor respective, şi le stochează pe mediul de stocare B, ancorând apoi aceste hash-uri la blockchain. Dacă C doreşte să şteargă date, nu poate să facă asta direct. Poate doar să trimită noi blocuri, în care datele respective nu mai sunt prezente, iar aceste blocuri vor fi adăugate de către A la brick-urile deja existente în B. Datele vor fi marcate ca şterse, dar vor fi prezente în continuare dacă vor fi căutate în brick-urile anterioare. Astfel, C nu mai are control direct asupra stocării datelor, ci poate doar accesa serviciile oferite de A, care nu includ ştergerea.

Un alt exemplu de realizare a invenţiei este prezentat în figura 7. Aici, sistemul de protecţie (A) este un sistem hardware accelerat, conectat la un server (C). Sistemul A este la rândul lui conectat la un sistem de stocare B. Sistemul de protecţie foloseşte în acest caz un sistem de control al versiunilor de tip "git". Când C trimite date spre a fi stocate, A verifică dacă datele respective există deja în sistemul de control al versiunilor. În caz că nu există, aceste date sunt adăugate. În caz că există deja, o nouă versiune este adăugată.

SC AQUASoft SRL

Rector,
Prof. Dr. Tudorel Toader

ROMÂNIA
UNIVERSITATEA „ALEXANDRU IOAN CUZA" DIN IAŞI
MINISTERUL EDUCAŢIEI

25

Un al treilea exemplu este prezentat în figura 8. Aici, sistemul de protecţie (A) este un dispozitiv conectat la calculatorul C prin USB, şi conectat de asemenea la un disc extern, tot prin USB. Sistemul de stocare este un simplu sistem de stocare a fişierelor de tip FAT. Când C trimite un fişier cu date spre a fi stocat, A verifică dacă fişierul respectiv există deja pe disc. În cazul în care acesta nu există, este adăugat. În caz că fişierul există deja, numele fişierului deja existent este modificat, adăugându-i-se de exemplu, pe lângă numele existent, un separator standard şi un cod cu data şi ora curentă. Noua versiune este apoi adăugată cu numele original.

SC AQUASoft SRL

Rector,
Prof. Dr. Tudorel Toader

24

REVENDICĂRI

1. Sistem de protectie a datelor prin prevenirea modificarilor acestora, **caracterizat prin aceea că:**
   previne modificările asupra datelor stocate sau ştergerea acestora, permiţând doar adăugarea de date noi sau de versiuni noi a datelor existente. Sistemul poate fi bazat pe oricare din mai multe tehnologii de stocare:
   - pe un sistem de fişiere normal, redenumind fişierele vechi atunci când se adaugă o versiune nouă.
   - pe un sistem de control al versiunilor, care păstrează versiuni anterioare ale datelor.
   - pe un sistem de blocuri de date ancorate în ledgere distribute (ca de exemplu blockchain).

Companie

Rector,
Prof. Dr. Tudorel Toader

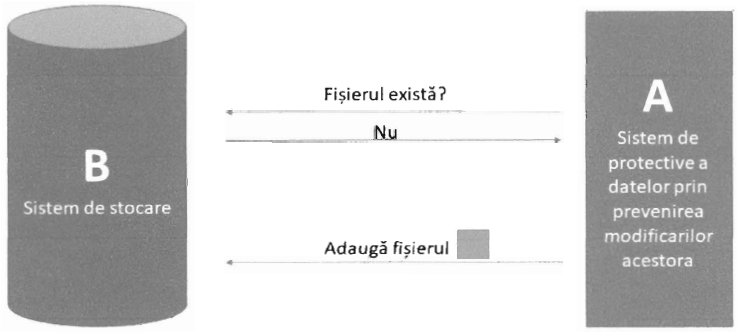

Figura 1. Funcționarea sistemului cu un sistem de fișiere standard când fișierul nu există deja.

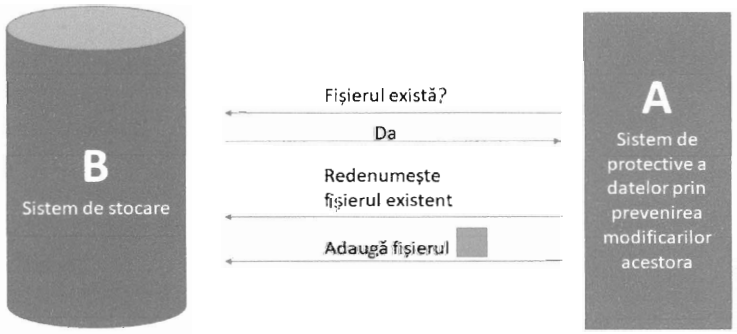

Figura 2. Funcționarea sistemului cu un sistem de fișiere standard când fișierul există deja.

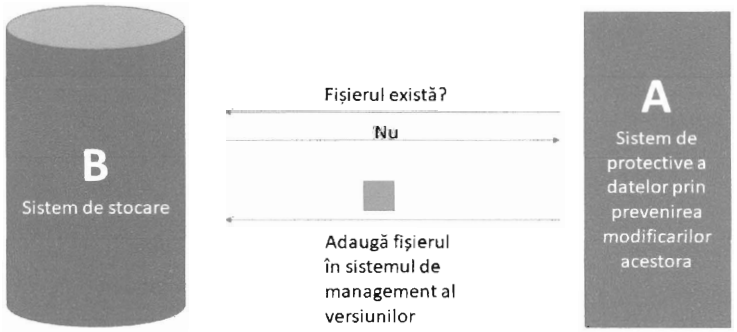

Figura 3. Funcționarea sistemului cu un sistem de control al versiunilor când fișierul nu există deja.

Companie

Rector,
Prof. Dr. Tudorel Toader

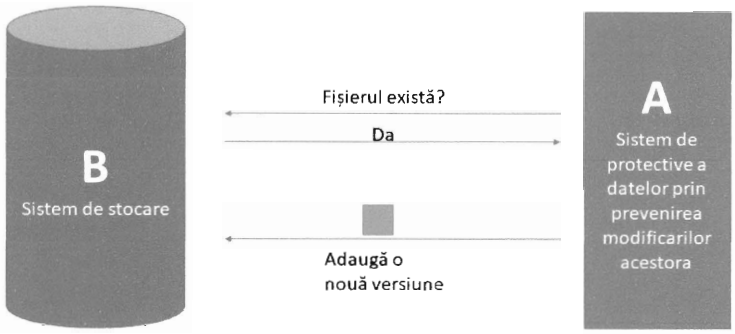

Figura 4. Funcționarea sistemului cu un sistem de control al versiunilor când fișierul există deja.

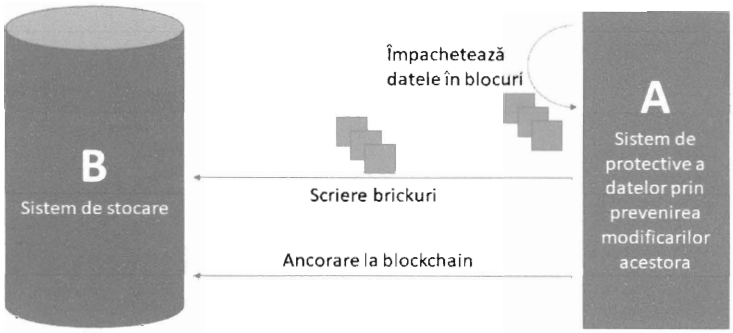

Figura 5. Funcționarea sistemului cu un sistem bazat pe blockchain.

Companie

Rector,
Prof. Dr. Tudorel Toader

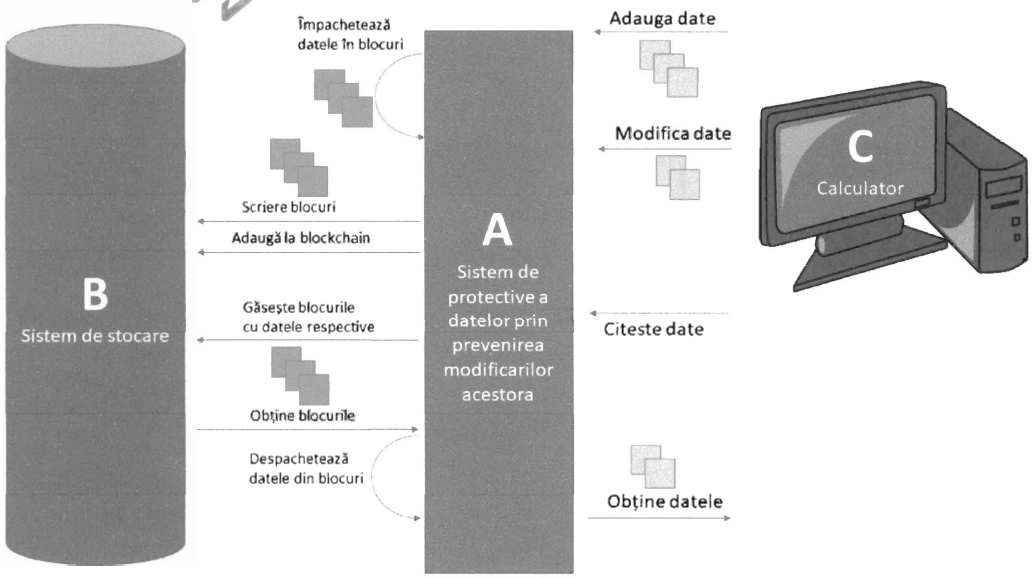

Figura 6. Exemplu de funcționare a sistemului bazat pe blocuri.

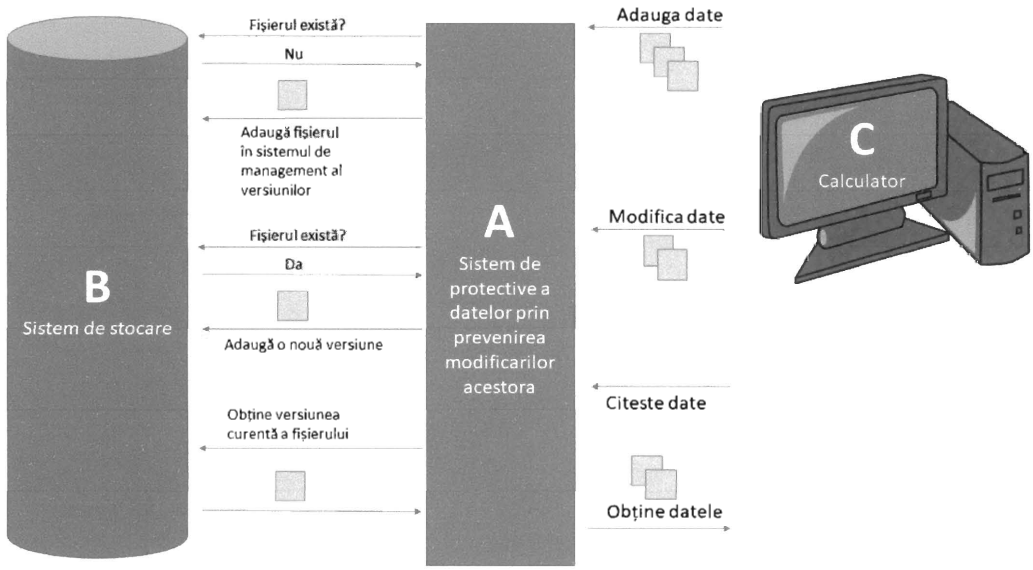

Figura 7. Exemplu de funcționare a sistemului bazat pe controlul versiunilor

Companie

Rector,
Prof. Dr. Tudorel Toader

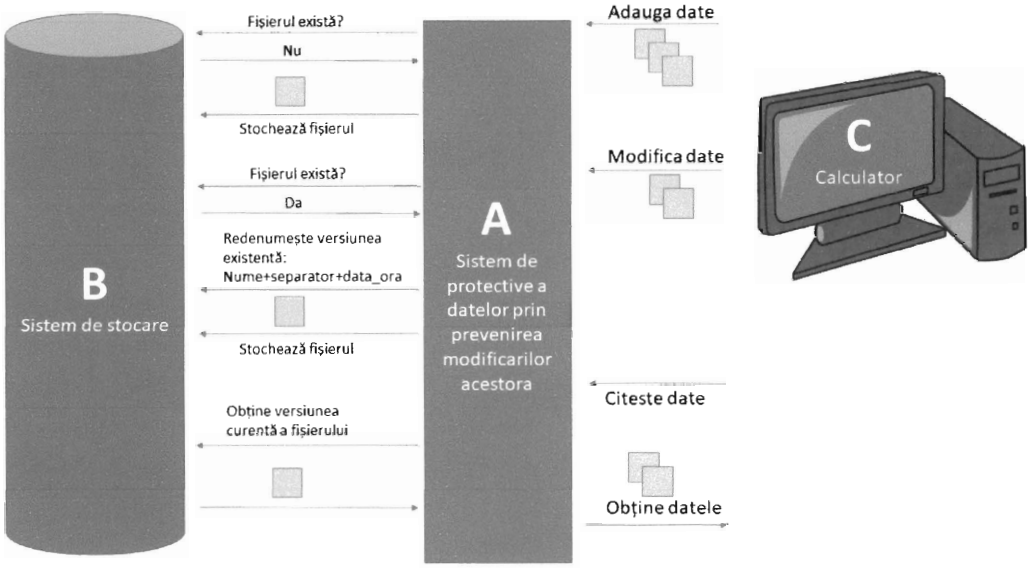

Figura 8. Exemplu de funcționare a sistemului bazat pe sistem de stocare a fișierelor

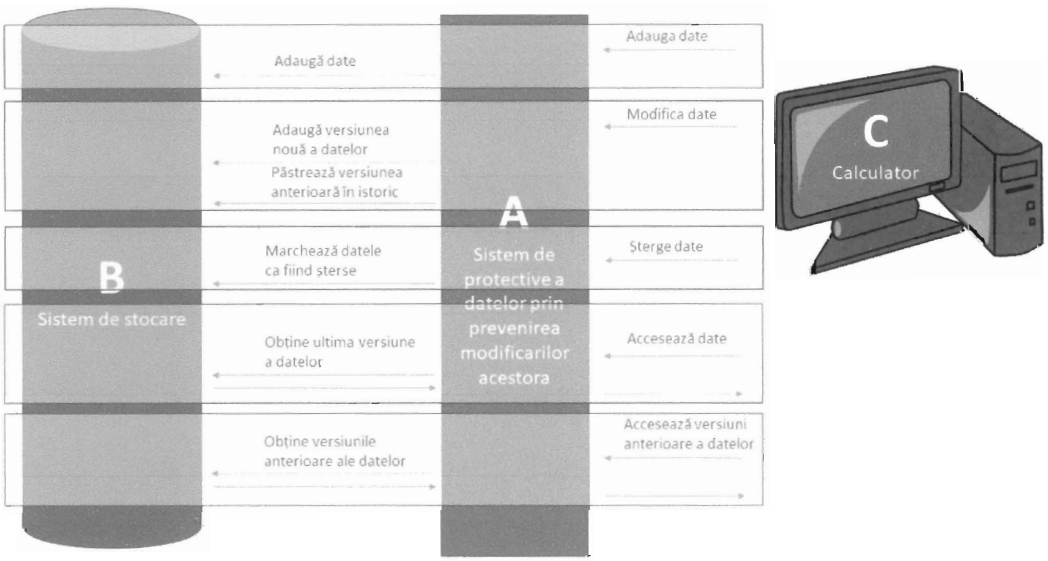

Figura 9. Operațiuni executate de către sistemul de protecție

Companie

Rector,
Prof. Dr. Tudorel Toader

REVENDICĂRI

1. Sistem de protecţie a datelor prin prevenirea modificarilor acestora, **caracterizat prin aceea că:**

Este un sistem fizic sau programatic, poziţionat ca o interfaţă între un sistem de calcul şi mediul de stocare. Sistemul de protecţie limitează în mod controlat numărul de operaţiuni asupra datelor, nepermiţând ştergerea sau modificarea directă a datelor. Sistemul de protectie permite doar adăugarea de date noi, sau versiuni noi ale datelor existente.

Sistemul de protecţie se poate aplica pentru mai multe tehnologii de stocare:

- pe un sistem de fişiere normal, redenumind fişierele vechi atunci când se adaugă o versiune nouă.
- pe un sistem de control al versiunilor, care păstrează versiuni anterioare ale datelor.
- pe un sistem de blocuri de date ancorate în registre distribute de date (ca de exemplu tehnologia blockchain).

Compania
Cristian Stoica

Rector
Prof. Dr. Tudorel Toader