MD 956 Z 2016.04.30

REPUBLICA MOLDOVA

(19) Agenţia de Stat
pentru Proprietatea Intelectuală

(11) **956** (13) **Z**
(51) **Int.Cl:** ***H04L 9/00*** (2006.01)
H04L 29/06 (2006.01)
H04K 1/00 (2006.01)

(12) BREVET DE INVENŢIE DE SCURTĂ DURATĂ

(21) Nr. depozit: s 2015 0017 **(22) Data depozit:** 2015.02.17	**(45) Data publicării hotărârii de acordare a brevetului:** 2015.09.30, BOPI nr. 9/2015

(71) Solicitant: SOCIETATEA CU RĂSPUNDERE LIMITATĂ "SIGURANŢĂ TRANZACŢII", MD
(72) Inventatori: FLORESCU Alexandru-Ion, RO; DUDUICA Simon, RO
(73) Titular: SOCIETATEA CU RĂSPUNDERE LIMITATĂ "SIGURANŢĂ TRANZACŢII", MD
(74) Mandatar autorizat: JENICICOVSCAIA Galina

(54) Metodă de prevenire a infracţiunii la solicitarea prestării de servicii prin intermediul reţelei Internet

(57) Rezumat:

Invenţia se referă la metode de prevenire a fenomenului infracţional potenţial existent la solicitarea din partea unui utilizator către furnizorul ce prestează servicii prin reţeaua Internet.

Metoda de prevenire a infracţiunii la solicitarea prestării de servicii prin intermediul reţelei Internet constă în aceea că la recepţionarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului şi suma de control a fişierului, de asemenea determinand datele specifice ale dispozitivului utilizatorului. In cazul imposibilităţii de identificare a datelor sus-numite, se stabileşte o conexiune suplimentară între serverul furnizorului şi dispozitivul utilizatorului, care execută o verificare pasivă, solicitând date suplimentare de autentificare.

Revendicări: 1
Figuri: 5

MD 956 Z 2016.04.30

(54) Method for offence prevention at the request of providing services by means of the Internet network

(57) Abstract:

1

The present invention relates to methods for preventing the potentially existing offence phenomenon at user's request to the service provider by means of the Internet network.

The method for offence prevention at the request of providing services by means of the Internet network consists in that upon entry of signal-request from the user device to the server of the provider to disclose the intruder, the server performs an active testing,

2

prompting the account data and fingerprint from the user, as well as identifying the specific data of user device. In case of failure to identify the above data, it is established a bypass connection between the server of the provider and the user device, which performs a passive testing, prompting additional authentication data.

Claims: 1

Fig.: 5

(54) Метод предотвращения правонарушения при запросе о предоставлении услуг посредством сети Интернет

(57) Реферат:

1

Изобретение относится к методам предотвращения потенциально существующего явления правонарушения при запросе со стороны пользователя к поставщику услуг посредством сети Интернет.

Метод предотвращения правонарушения при запросе о предоставлении услуг посредством сети Интернет состоит в том, что при поступлении сигнала-запроса с устройства пользователя на сервер провайдера для раскрытия злоумышленника, сервер осуществляет активную

2

проверку, запрашивая у пользователя данные аккаунта и контрольную сумму файла, а также определив специфические данные устройства пользователя. В случае невозможности идентификации вышеперечисленных данных, устанавливается дополнительное соединение между сервером провайдера и устройством пользователя, которое выполняет пассивную проверку, запрашивая дополнительные данные аутентификации.

П. формулы: 1

Фиг.: 5

Descriere:

Invenţia se referă la metode de prevenire a fenomenului infracţional potenţial existent la solicitarea din partea unui utilizator către furnizorul ce prestează servicii prin reţeaua Internet.

Metoda poate fi utilizată în cadrul prestării următoarelor servicii, fără a se limita la acestea:

- servicii care presupun autentificarea clientului prin intermediul unei metode de autentificare alese de furnizorul de servicii;
- servicii care presupun autentificarea clientului prin intermediul unei metode de autentificare alese de furnizorul de servicii şi necesită o limitare cantitativă a serviciului prestat (exemplu: free trial);
- servicii care nu presupun autentificarea clientului şi necesită o limitare cantitativă a serviciului prestat (exemplu: accesul trebuie să fie restricţionat la un număr maxim de accesări zilnice de către un singur utilizator);
- din punct de vedere al bunului oferit, servicii exclusiv online din tipurile de mai sus;
- servicii care presupun furnizarea unui bun tangibil ca urmare a unei comenzi efectuate prin intermediul interfeţei electronice a serviciului.

Este cunoscută o metodă de prevenire a infracţiunii la solicitarea prestării de servicii prin intermediul reţelei Internet, care constă în aceea că la recepţionarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului, ID-ul atribuit de sistemul de prevenire a fraudei pentru dispozitivul client al utilizatorului (device ID), amprenta digitală a dispozitivului client (generată de către sistemul antifraudă pe baza informaţiilor specifice ale dispozitivului client la accesarea serviciului), suma de control a fişierului, de asemenea determinând datele specifice ale dispozitivului utilizatorului, cookie, ID-ul sesiunii şi introducându-le pe acestea in memoria sa [1].

Dezavantajele acestei metode constau in aceea că astfel de metode de verificare a datelor utilizatorului pot fi vulnerabile, deoarece există situaţii, când serverul furnizorului nu poate identifica ID-ul utilizatorului, cum ar fi situaţii în care dispozitivul nu permite stocarea ID-ului sau cand utilizatorul a şters acest ID ca urmare a unei operaţiuni de mentenanţă a dispozitivului sau situaţii în care furnizorul de servicii nu doreşte stocarea ID-ului datorită contextului în care oferă serviciu. In cazul in care serverul furnizorului nu poate identifica ID-ul utilizatorului, sistemul refuză de a presta utilizatorului serviciul solicitat. Însă în cazul în care utilizatorul, care a solicitat serviciul, este un utilizator de bună credinţă, iar sistemul furnizorului nu poate identifica ID-ul calculatorului acestuia, apare situaţia, în care furnizorul refuză prestarea serviciului unui utilizator de bună credinţă.

Problema pe care o rezolvă invenţia constă în crearea unei metode, care ar asigura autentificarea securizată pentru utilizator şi optimizarea interacţiunii utilizator-furnizor în ceea ce priveşte eficacitatea şi siguranţa.

Metoda, conform invenţiei, înlătură dezavantajele menţionate mai sus prin aceea că la recepţionarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului şi suma de control a fişierului, de asemenea determinând datele specifice ale dispozitivului utilizatorului, cookie, ID-ul sesiunii şi introducându-le pe acestea in memoria sa, in cazul imposibilităţii de identificare a datelor accountului utilizatorului sau sumei de control a fişierului utilizatorului, se stabileşte o conexiune suplimentară între serverul furnizorului şi dispozitivul utilizatorului, care execută o verificare pasivă, solicitand date suplimentare de autentificare.

Invenţia se explică prin desenele din figurile 1-5, care reprezintă:

- fig. 1, schema legăturilor între dispozitivul utilizatorului şi furnizor;
- fig. 2, schema generală de parcurs a semnalului solicitării din start până la accesul serviciului, sau refuzul definitiv de prestare a serviciului, incluzand detalii pentru investigarea preliminară;
- fig. 3, schema parcursului semnalului solicitării în cadrul verificării pasive;

- fig. 4, schema parcursului semnalului solicitării în cadrul verificării active a unui dispozitiv cu indicator dispozitiv prezent;
- fig. 5, schema parcursului semnalului solicitării în cadrul verificării active a unui dispozitiv fără identificator dispozitiv prezent, cu recurs la investigarea pasivă.

Lista semnelor convenţionale:

DC : dispozitiv client

CD1 : context dispozitiv 1 - de exemplu referrer şi informaţii de genul acesta

CD2 : context dispozitiv 2 - de exemplu dacă ADC a putut fi salvată pe dispozitiv

CD3 : context dispozitiv 3 - de exemplu adresa IP, resursa (URL)

ADD : amprenta digitală dispozitiv (calcularea ei se face pe baza caracteristicilor dispozitivului)

ID: identificator dispozitiv - este un identificator unic generat de către SPF şi salvat pe DC

ADC : aplicaţie detecţie client

SP : sistem prevenire

BD-SP : baza de date - sistem prevenire

ADF : aplicaţie de detecţie furnizor

FS : furnizor de servicii

FS-CPC : furnizor de servicii - configurare punct de control

RDFS : reguli definite de către furnizorul de servicii

AC : aplicaţie cadru a furnizorului de servicii (javascript)

ICU : informaţii comportament utilizator

DIU : datele introduse de către utilizator - setul de date ce trebuie introduse de către utilizatorul care accesează un anume serviciu/resursă. Pot fi datele de acces (login) sau de inscriere

DRDA : Date Relevante pentru Domeniul de Activitate.

Metoda propusă constă în aceea că la recepţionarea semnalului-solicitare de la dispozitivul infractorului presupus (1) (in figura 1) de serverul furnizorului (2), serverul solicită de la utilizator informaţia privind contul acestuia şi amprenta digitală a dispozitivului client (fingerprint) şi introduce aceste date în memoria sa, după care utilizatorul completează formularul de solicitare a serviciului, in cazul in care modalitatea de acces a serviciului stabilită de furnizor prevede acest pas. In această etapă se realizează o verificare activă a conştiinciozităţii utilizatorului prin determinarea datelor specifice ale dispozitivului utilizatorului, cum ar fi modul cookie, sesiunea ID, etc. In cazul in care dispozitivul utilizatorului nu a trecut verificarea activă, adică serverul furnizorului nu a reuşit citirea informaţiei cu privire la contul sau la amprenta digitală a dispozitivului client al utilizatorului, se conectează automat legătura suplimentară între serverul furnizorului şi dispozitivul utilizatorului, care execută o verificare pasivă, folosind datele disponibile la momentul respectiv.

Schema legăturilor între dispozitivul utilizatorului şi furnizor (figura 1)

Diagrama reprezintă schematic interacţiunea dintre un utilizator şi un formular al unui furnizor de servicii. Utilizatorul accesează o pagină web, unde furnizorul de servicii prezintă nişte câmpuri care trebuie completate. În pagina web este prezentă şi aplicaţia detectare infractor client (denumită în cele ce urmează "aplicaţie de detecţie client") servită de către sistemul de prevenire a infracţionalităţii din cadrul invenţiei (denumit în cele ce urmează "sistem de prevenire") care face o sumă de verificări pe dispozitiv client. Odată făcute aceste verificări, clientul contactează sistemul de prevenire şi-i trimite datele de amprentare digitală pasivă bazate pe datele culese de pe dispozitivul client. De asemenea se transmit şi date de genul cookies sau identificator de device, acesta din urmă în cazul în care verificarea activă este posibilă. În momentul în care utilizatorul trimite formularul completat pe dispozitivul client, datele completate de către utilizator împreună cu amprenta digitală dispozitiv sunt trimise la furnizorul de servicii. Furnizorul de servicii trimite mai departe la sistemul de prevenire date cum ar fi amprenta digitală, dispozitiv şi informaţii de identificare şi primeşte înapoi un scor pe baza căruia este evaluată credibilitatea clientului.

Procedura de verificare pe etape se realizează în modul ce urmează.

Etapa investigării preliminare (figura 2)

De la dispozitivul utilizatorului se expediază o solicitare spre serverul furnizorului. Serverul furnizorului răspunde acestei solicitări transmiţând aplicaţia cadru (denumită în cele ce urmează "aplicaţie cadru") pentru furnizarea serviciului. Aplicaţia cadru este o aplicaţie specifică furnizorului de servicii care permite utilizatorului să acceseze serviciul intr-o etapă ulterioară. Această aplicaţie cadru este integrată cu aplicaţia detecţie client furnizată de sistemul de prevenire. Aplicaţia cadru lansează aplicaţia de detecţie client pe dispozitivul utilizatorului. Dacă lansarea a eşuat, sistemul de prevenire nu va putea realiza verificarea şi, prin urmare, accesul utilizatorului la serviciul respectiv va fi refuzat. Dacă lansarea este reuşită, în funcţie de configurările specifice realizate de furnizorul de servicii pentru punctul de control, se va proceda în felul următor: (a) dacă punctul de control este configurat ca punct de control cu verificare doar pasivă, se va proceda la realizarea identificării pasive (figura 3); şi (b) dacă punctul de control necesită verificare completă, se va proceda la citirea identificatorului dispozitiv şi la generarea amprentei dispozitiv. Ca o continuare la opţiunea descrisă la litera (b) din propoziţia precedentă, dacă identificatorul dispozitiv este găsit, se va continua cu paşii descrişi în figură (figura 4), iar dacă identificatorul dispozitiv nu este găsit, se va continua cu paşii descrişi în figură (figura 5).

Etapa investigării complete, varianta investigării pasive pentru prevenirea fraudei (figura 3)

Se continuă din figura 2. Pe dispozitivul clientului se generează amprenta dispozitivului, pe baza datelor specifice disponibile pe dispozitiv, cum ar fi, dar nelimitandu-se la: tip de browser, limbă, sistem de operare, tipuri de caractere, module instalate, etc. Dacă nu este necesar ca utilizatorul să introducă date de acces intr-un formular, atunci amprenta dispozitivului se trimite la furnizorul de servicii. Dacă este nevoie ca utilizatorul să introducă date suplimentare, atunci aplicaţia cadru va afişa un formular pe dispozitivul client. În timp ce clientul introduce datele, aplicaţia de detecţie client colectează informaţiile de comportament ale utilizatorului care apoi împreună cu datele introduse de utilizator şi amprenta dispozitiv sunt trimise la furnizorul de servicii. Furnizorul de servicii validează mai întâi datele introduse de către utilizator; dacă nu sunt valide/bune şi este permisă o nouă încercare de introducere a datelor, utilizatorului îi va fi afişat din nou formularul pe dispozitivul client. Dacă însă datele introduse de către utilizator sunt valide, atunci aplicaţia de detecţie pentru furnizorul de servicii (denumită în cele ce urmează "aplicaţia de detecţie furnizor") adună datele din contextul dispozitiv 3 (de exemplu adresa IP, resursa (URL) denumită în cele ce urmează "context dispozitiv 3") şi le trimite la sistemul de prevenire, împreună cu informaţiile de comportament şi amprenta dispozitiv primite de la aplicaţia de detecţie client. Aplicaţia de detecţie furnizor este o aplicaţie furnizată de sistemul de prevenire şi integrată cu sistemul furnizorului de servicii. Sistemul de prevenire determină, pe baza algoritmului de investigare pasivă şi a datelor primite, dacă există înregistrări care atestă, cu o probabilitate prestabilită, faptul că dispozitivul este identic cu dispozitive conectate anterior. Sistemul de prevenire evaluează datele disponibile (informaţiile dispozitivelor determinate a fi identice, datele introduse de către utilizator, amprenta dispozitiv, informaţiile comportament utilizator, contextul dispozitiv 1, contextul dispozitiv 3, datele de identificare domeniu de activitate) pe baza regulilor definite de către furnizorul de servicii în interfaţa de administrare a sistemului de prevenire şi pe baza datelor relevante pentru domeniul de activitate respectiv, adunate de sistemul de prevenire de la ceilalţi furnizori de servicii. În urma evaluării datelor de mai sus de către sistemul de prevenire, acesta răspunde către furnizorul de servicii transmiţând o recomandare (acceptă, respinge sau analizează), un scor, precum şi informaţii despre regulile care au fost aplicate pentru obţinerea scorului. În cazul recomandării acceptă, furnizorul de servicii va pune la dispoziţie resursa pe care utilizatorul doreşte s-o acceseze, prin intermediul aplicaţiei cadru de pe dispozitivul client. În cazul recomandării respinge sau analizează, furnizorul de servicii poate afişa informaţii privitoare la accesul restricţionat prin intermediul aplicaţiei cadru de pe dispozitivul client. În cazul recomandării analizează, administratorul furnizorului

de servicii este notificat şi va putea ulterior accepta sau respinge manual cererea din interfaţa de administrare a sistemului de prevenire. La o accesare ulterioară de către utilizator a resursei sau serviciului, sistemul de prevenire va emite recomandarea acceptă sau respinge, corespunzător cu acţiunea manuală a administratorului.

Etapa investigării complete, varianta investigării active pentru prevenirea fraudei, a unui dispozitiv cu identificator dispozitiv prezent (figura 4)

Se continuă din figura 2. Dacă nu este necesar ca utilizatorul să introducă date de acces intr-un formular, atunci amprenta dispozitivului, împreună cu identificatorul de dispozitiv se trimite la furnizorul de servicii. Dacă este nevoie ca utilizatorul să introducă date suplimentare, atunci aplicaţia cadru va afişa un formular pe dispozitivul client. În timp ce clientul introduce datele, aplicaţia de detecţie client colectează informaţiile de comportament ale utilizatorului care apoi împreună cu datele introduse de utilizator, identificatorul de dispozitiv şi amprenta dispozitiv sunt trimise la furnizorul de servicii. Acesta validează mai întâi datele introduse de către utilizator; dacă nu sunt valide/bune şi este permisă o nouă încercare de introducere a datelor, utilizatorului îi va fi afişat din nou formularul pe dispozitivul client. Dacă însă datele introduse de către utilizator sunt valide, atunci aplicaţia de detecţie client pentru furnizorul de servicii adună datele context dispozitiv 3 şi le trimite sistemului de prevenire, împreună cu informaţiile de comportament şi amprenta dispozitiv primite de la aplicaţia de detecţie client. Aplicaţia de detecţie client pentru furnizorul de servicii este o aplicaţie furnizată de sistemul de prevenire şi integrată cu sistemul furnizorului de servicii. Sistemul de prevenire evaluează datele disponibile (datele introduse de către utilizator, identificatorul dispozitiv, amprenta dispozitiv, informaţiile comportament utilizator, contextul dispozitiv 1, contextul dispozitiv 3, datele de identificare domeniu de activitate) pe baza regulilor definite de către furnizorul de servicii în interfaţa de administrare a sistemului de prevenire şi pe baza datelor relevante pentru domeniul de activitate respectiv, adunate de sistemul de prevenire de la ceilalţi furnizori de servicii. În urma evaluării datelor de mai sus de către sistemul de prevenire, acesta răspunde către furnizorul de servicii transmiţând o recomandare (acceptă, respinge sau analizează), un scor, precum şi informaţii despre regulile care au fost aplicate pentru obţinerea scorului. În cazul recomandării acceptă, furnizorul de servicii va pune la dispoziţie resursa pe care utilizatorul doreşte s-o acceseze, prin intermediul aplicaţiei cadru de pe dispozitivul client. În cazul recomandării respinge sau analizează, furnizorul de servicii poate afişa informaţii privitoare la accesul restricţionat prin intermediul aplicaţiei cadru de pe dispozitivul client.

Etapa investigării complete, varianta investigării active pentru prevenirea fraudei, a unui dispozitiv fără identificator dispozitiv prezent, cu recurs la investigarea pasivă (figura 5)

Se continuă din figura 2. Pe dispozitivul clientului se generează amprenta dispozitivului, pe baza datelor specifice disponibile pe dispozitiv, la fel ca la figura 3. Se transmite această amprentă către sistemul de prevenire, opţional prin intermediul unui serviciu de redirecţie furnizor (proxy) care are rolul de a face posibilă tranzacţionarea integrală prin intermediul furnizorului de servicii. Sistemul de prevenire, la primirea amprentei dispozitiv va genera identificatorul dispozitiv, va stoca amprenta dispozitiv împreună cu identificatorul dispozitiv şi informaţiile din contextul dispozitiv 1 (cum ar fi referrer şi informaţii de acest gen) şi va transmite către aplicaţia de detecţie client identificatorul dispozitiv. Aplicaţia de detecţie client va incerca stocarea identificatorului de dispozitiv pe dispozitiv, marcand in contextul dispozitiv 2, dacă această stocare s-a efectuat cu succes. Dacă nu este necesar ca utilizatorul să introducă date de acces într-un formular, atunci amprenta dispozitivului, împreună cu identificatorul de dispozitiv, se trimite la furnizorul de servicii. Dacă este nevoie ca utilizatorul să introducă date suplimentare, atunci aplicaţia cadru va afişa un formular pe dispozitivul client. În timp ce clientul introduce datele, aplicaţia de detecţie client colectează informaţiile de comportament ale utilizatorului care apoi împreună cu datele introduse de utilizator, identificatorul de dispozitiv şi amprenta dispozitiv sunt trimise la furnizorul de servicii. Ultimul validează mai întâi datele introduse de către utilizator; dacă nu sunt valide/bune şi este permisă o nouă încercare de introducere a datelor, utilizatorului îi va fi afişat din

nou formularul pe dispozitivul client. Dacă însă datele introduse de către utilizator sunt valide, atunci aplicaţia de detecţie furnizor adună datele pentru contextul dispozitiv 3 şi le trimite sistemului de prevenire, împreună cu contextul dispozitiv 2 (cum ar fi dacă de exemplu aplicaţie detecţie client a putut fi salvată pe dispozitiv), informaţiile de comportament şi amprenta dispozitiv primite de la aplicaţia de detecţie client. Sistemul de prevenire determină, pe baza algoritmului de investigare pasivă şi a datelor primite, dacă există înregistrări care atestă, cu o probabilitate prestabilită, faptul că dispozitivul este identic cu dispozitive conectate anterior. Acest pas este practic recursul la investigarea pasivă pentru un dispozitiv căruia i-a fost eliminat identificatorul dispozitiv de la ultima verificare. Apoi, sistemul de prevenire a fraudei evaluează datele disponibile (informaţiile dispozitivelor determinate a fi identice, datele introduse de către utilizator, amprenta dispozitiv, informaţiile comportament utilizator, contextul dispozitiv 1, contextul dispozitiv 3, date de relevanţe domeniu de activitate) pe baza regulilor definite de către furnizorul de servicii în interfaţa de administrare a sistemului de prevenire şi pe baza datelor relevante pentru domeniul de activitate respectiv, adunate de sistemul de prevenire de la ceilalţi furnizori de servicii. În urma evaluării datelor de mai sus de către sistemul de prevenire, acesta răspunde către furnizorul de servicii transmiţând o recomandare (acceptă, respinge sau analizează), un scor, precum şi informaţii despre regulile care au fost aplicate pentru obţinerea scorului. În cazul recomandării acceptă, furnizorul de servicii va pune la dispoziţie resursa pe care utilizatorul doreşte s-o acceseze, prin intermediul aplicaţiei cadru de pe dispozitivul client. În cazul recomandării respinge sau analizează, furnizorul de servicii poate afişa informaţii privitoare la accesul restricţionat prin intermediul aplicaţiei cadru de pe dispozitivul client.

În continuare se prezintă două exemple de folosire a metodei de prevenire a fraudei.

Primul exemplu se referă la o situaţie în care furnizorul de servicii online doreşte o identificare preferabil prin metoda activă a utilizatorului, acesta accesând serviciul pe baza unui cont, folosind login şi parola pentru autentificare. Astfel furnizorul oferă un serviciu online (denumit în cele ce urmează "SO") care pune la dispoziţia utilizatorilor facilităţi de procesare în cloud. Utilizatorul are avantajul că în loc să aibă nevoie de câteva săptămâni să genereze un film de animaţie poate face acest lucru în câteva ore/o zi. Folosind metoda care face obiectul invenţiei, un utilizator care incearcă să se înscrie a doua oară va fi identificat chiar şi în cazul în care foloseşte un alt cont sau chiar un alt dispozitiv de reţea din aceeaşi locaţie. Pe baza regulilor stabilite de către administratorii SO înscrierea/accesarea repetată a unui asemenea utilizator a site-ului poate genera o alertă în sistem. De asemenea în cazul in care dispozitivul utilizatorului nu permite stocarea unui identificator de dispozitiv sau acest identificator a fost eliminat, in urma investigării pasive, sistemul poate decide să îi permită accesul în cont, dar să nu-i ofere niciun beneficiu sau alternativă, să nu-i blocheze accesul, dacă este cunoscut de sistemul de prevenire ca un utilizator care a făcut fraudă prin intermediul cardurilor de credit în alte împrejurări. În felul acesta SO nu suferă pierderi din cauza utilizatorilor fraudulenţi şi îşi poate mări în acelaşi timp vânzările.

Al doilea exemplu se referă la o publicaţie online care funcţionează pe bază de abonament, dar permite accesul neautentificat al unui vizitator la un articol pe zi. Această politică este implementată în scopul de a atrage cititorii şi a-i convinge prin calitatea materialelor să dorească să citească mai mult şi, prin urmare, să îşi facă abonament. Însă această politică implică posibilitatea limitării accesului fără a recurge la un cont de utilizator. Folosind sistemul de prevenire prin metoda pasivă a acestuia, în condiţiile în care nu se doreşte stocarea unui identificator de dispozitiv pe un dispozitiv cu al cărui posesor nu este într-o relaţie contractuală, publicaţia online poate identifica in mod unic un dispozitiv sau chiar cu o probabilitate suficient de bună un utilizator care foloseşte dispozitive din aceeaşi locaţie şi, prin urmare, poate limita accesul la un articol pe zi şi astfel obţine venituri din abonamente în timp ce implementează politica de mai sus pentru atragerea clienţilor.

(56) Referinţe bibliografice citate in descriere:

1. US 7330871 B2 2008.02.12

(57) Revendicări:

Metodă de prevenire a infracţiunii la solicitarea prestării de servicii prin intermediul reţelei Internet, care constă în aceea că la recepţionarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului şi suma de control a fişierului, de asemenea determinand datele specifice ale dispozitivului utilizatorului, cookie, ID-ul sesiunii şi introducându-le pe acestea in memoria sa, **caracterizată prin aceea că** in cazul imposibilităţii de identificare a datelor accountului utilizatorului sau sumei de control a fişierului utilizatorului, se stabileşte o conexiune suplimentară între serverul furnizorului şi dispozitivul utilizatorului, care execută o verificare pasivă, solicitand date suplimentare de autentificare.

Şef adjunct Direcţie Brevete : IUSTIN Viorel

Şef Secţie Examinare: LEVIŢCHI Svetlana

Examinator: GHIŢU Irina

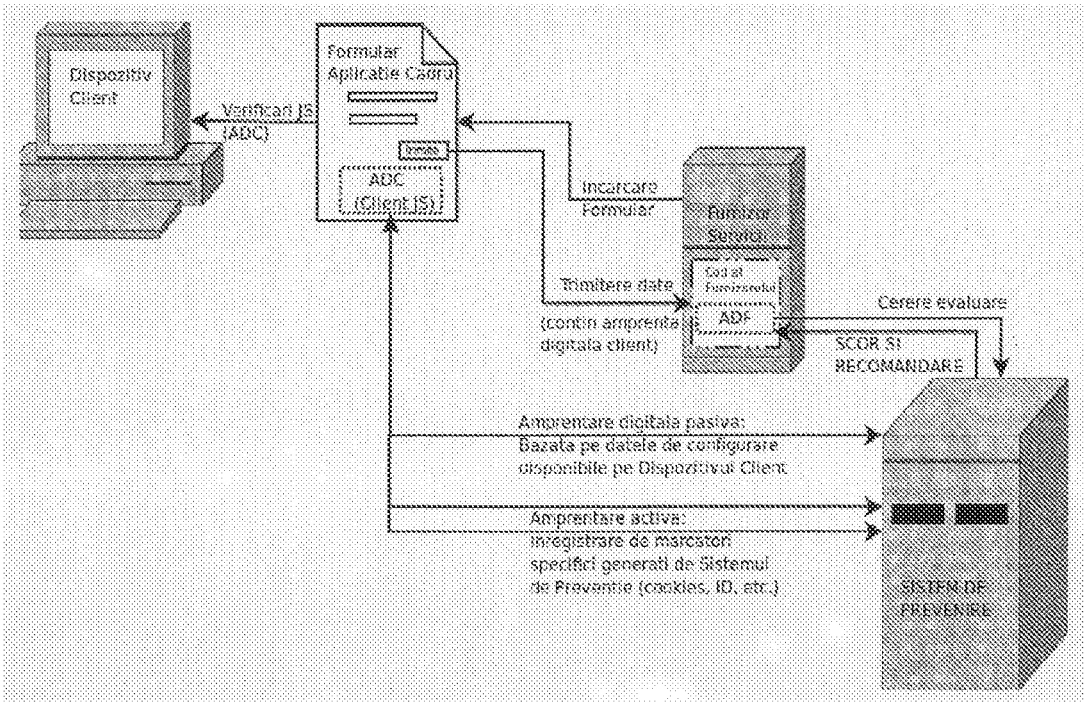
Dispozitiv Client
Formular Aplicatie Cadru
Verificari (S) (ADC)
ADC (Client JS)
Incarcare Formular
Furnizor Servicii
Trimitere date (contin amprenta digitala client)
ADF
Cerere evaluare
SCOR SI RECOMANDARE
Amprentare digitala pasiva: Bazata pe datele de configurare disponibile pe Dispozitivul Client
Amprentare activa: Inregistrare de marcatori specifici generati de Sistemul de Prevenire (cookies, ID, etc.)
SISTEM DE PREVENIRE

Fig. 1

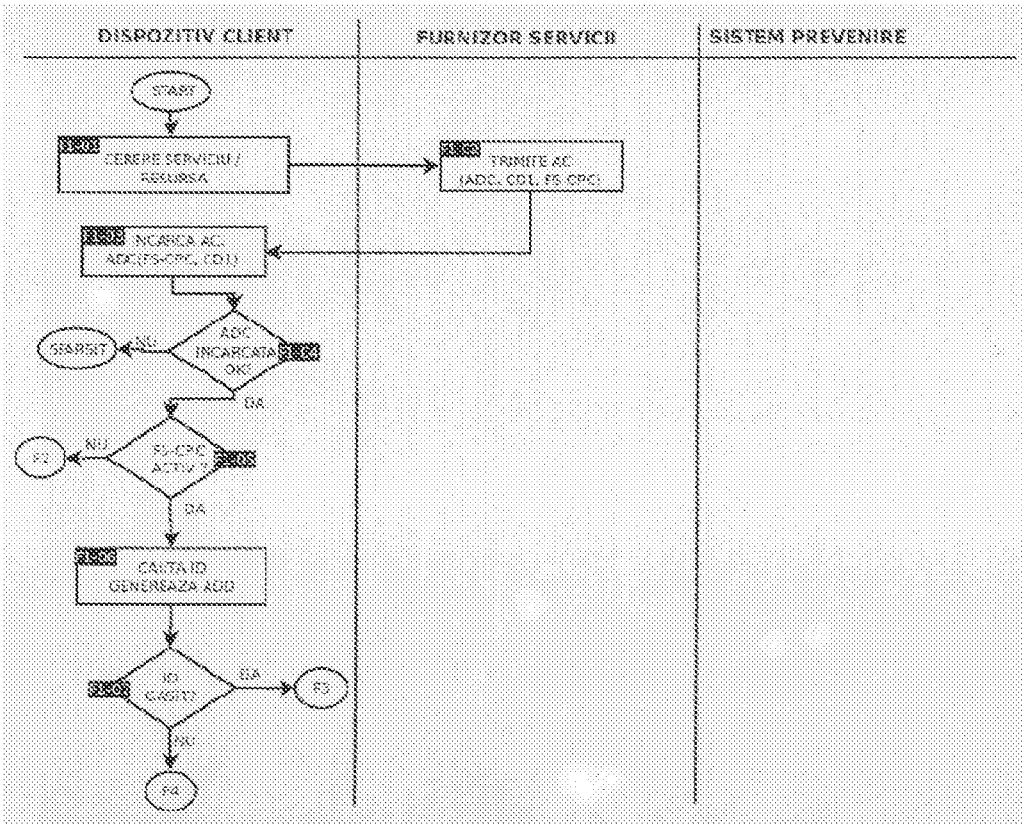
DISPOZITIV CLIENT
FURNIZOR SERVICII
SISTEM PREVENIRE
START
CERERE SERVICIU / RESURSA
TRIMITE AC (ADC, CDL, FS CPC)
INCARCA AC ADC(FS-CPC, CDL)
ADC INCARCATA OK?
START
NU
DA
FS
NU
FS-CPC ACTIV ?
DA
CAUTA ID GENEREAZA ADID
ID CASTIG?
DA
FS
NU
FS

Fig. 2

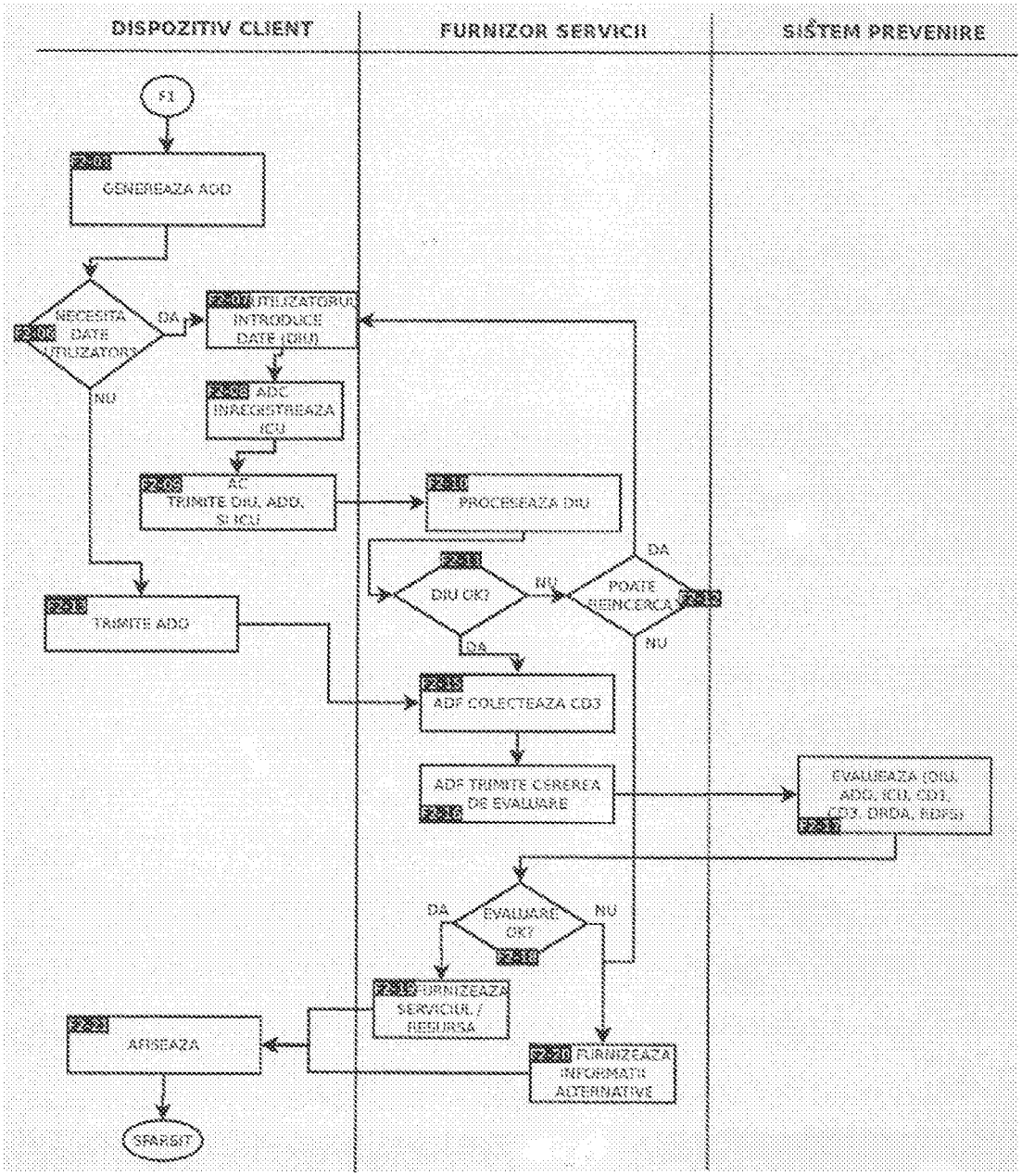
DISPOZITIV CLIENT
FURNIZOR SERVICII
SISTEM PREVENIRE
F1
GENEREAZA ADD
NECESITA DATE UTILIZATOR?
DA
NU
UTILIZATORUL INTRODUCE DATE (DIU)
ADC INREGISTREAZA (C1)
AC TRIMITE DIU, ADD, SI IC1
PROCESEAZA DIU
DIU OK?
NU
POATE REINCERCA
DA
NU
DA
TRIMITE ADD
ADF COLECTEAZA CD3
ADF TRIMITE CEREREA DE EVALUARE
EVALUEAZA (DIU, ADD, IC1, CD1, CD3, DRDA, RDFS)
EVALUARE OK?
DA
NU
FURNIZEAZA SERVICIUL / RESURSA
FURNIZEAZA INFORMATII ALTERNATIVE
AFISEAZA
SFARSIT

Fig. 3

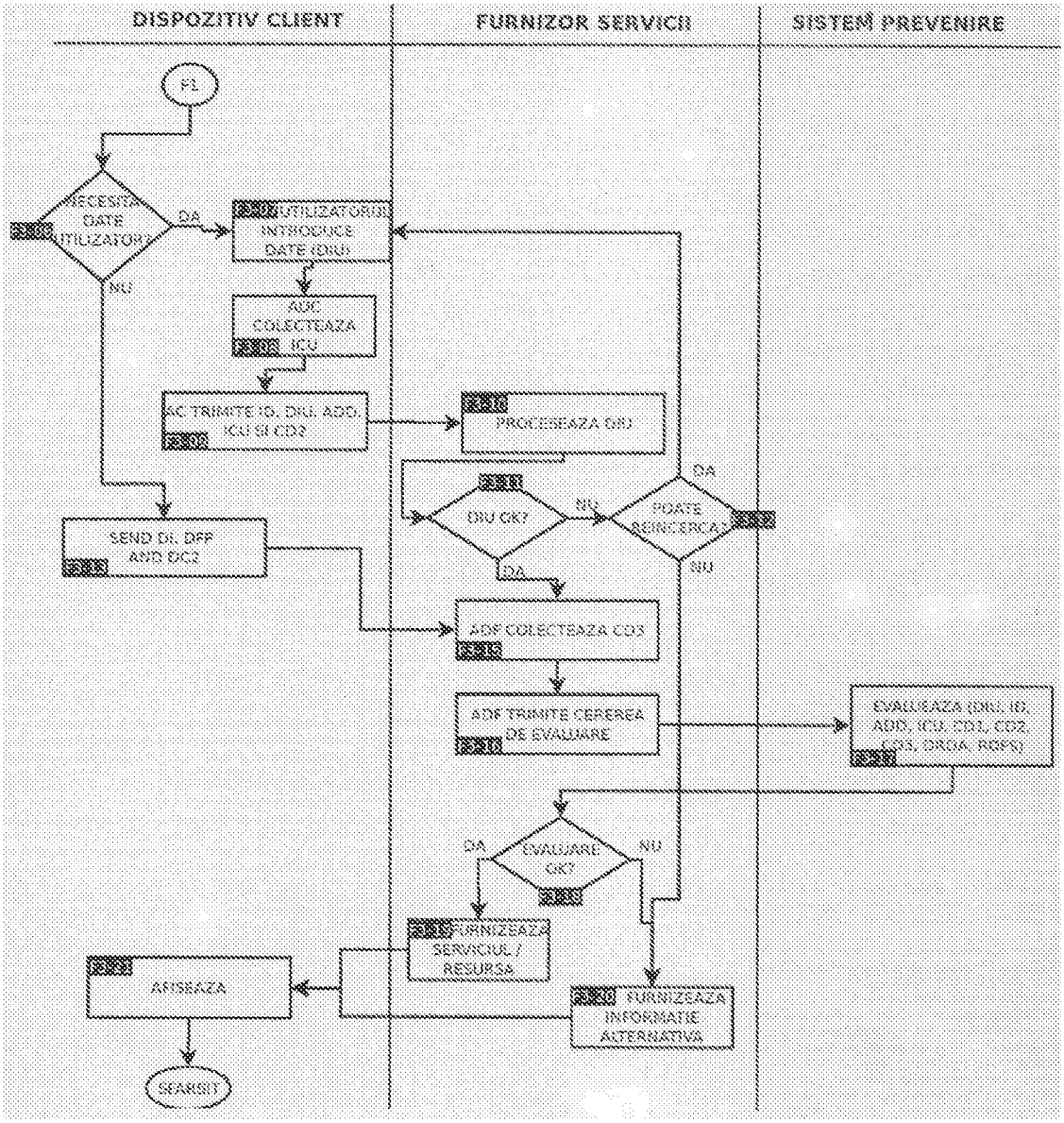
DISPOZITIV CLIENT
FURNIZOR SERVICII
SISTEM PREVENIRE
S1
NECESITA DATE UTILIZATOR?
DA
NU
UTILIZATORUL INTRODUCE DATE (DIU)
ADF COLECTEAZA ICU
SC TRIMITE ID, DIU, ADD, ICU SI CD2
PROCESEAZA DIU
DIU OK?
NU
POATE REINCERCA?
DA
NU
DA
SEND DIU, DFP AND DC2
ADF COLECTEAZA CD3
ADF TRIMITE CEREREA DE EVALUARE
EVALUEAZA (DIU, ID, ADD, ICU, CD1, CD2, CD3, DRDA, RDFS)
EVALUARE OK?
DA
NU
FURNIZEAZA SERVICIUL / RESURSa
AFISEAZA
FURNIZEAZA INFORMATIE ALTERNATIVA
SFARSIT

Fig. 4

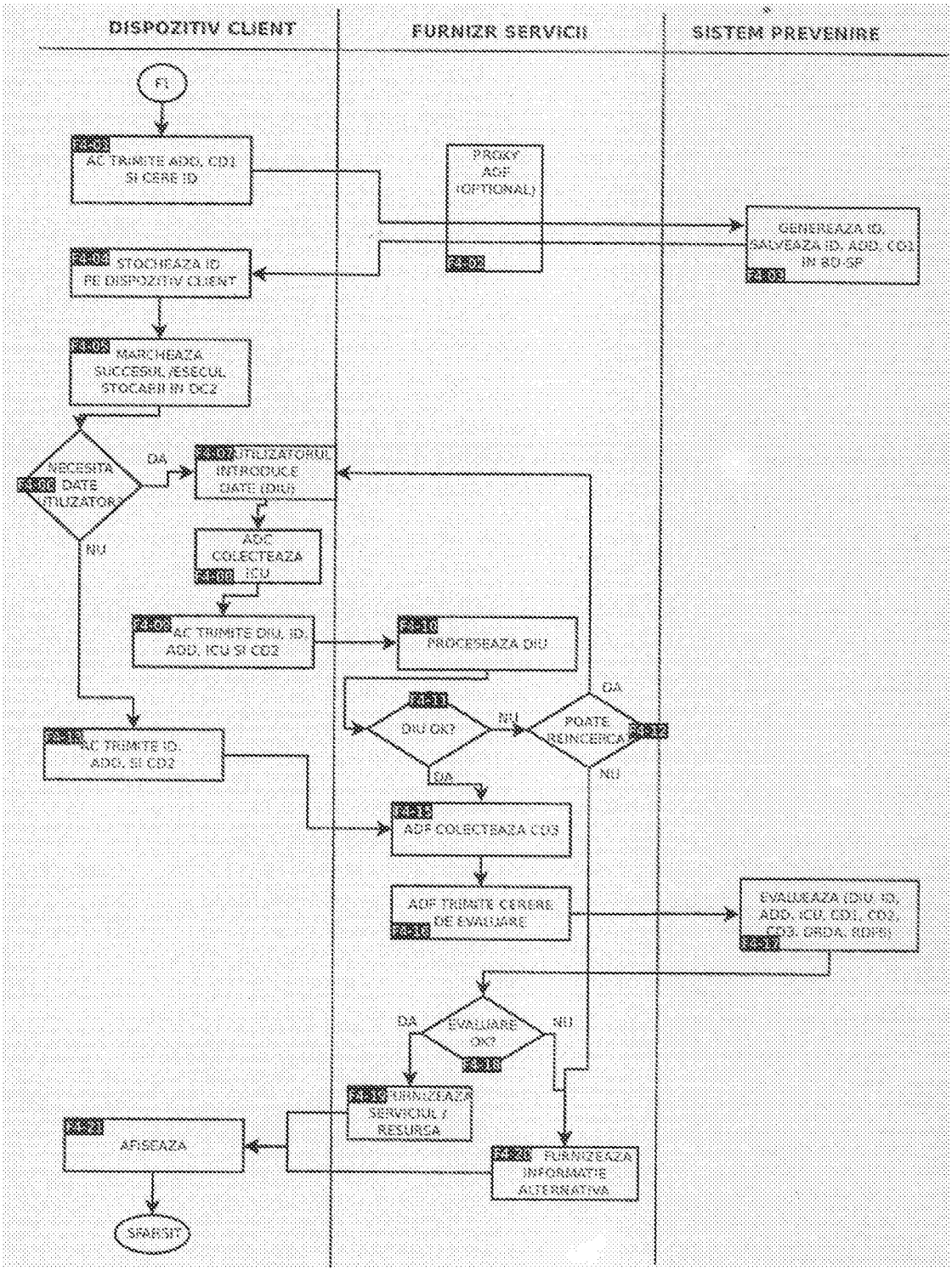
DISPOZITIV CLIENT
FURNIZOR SERVICII
SISTEM PREVENIRE
F1
AC TRIMITE ADD, CD1 SI CERE ID
PROXY ADF (OPTIONAL)
GENEREAZA ID, SALVEAZA ID, ADD, CD1 IN BD-SP
STOCHEAZA ID PE DISPOZITIV CLIENT
MARCHEAZA SUCCESUL /ESECUL STOCARII IN DC2
NECESITA DATE UTILIZATOR
DA
UTILIZATORUL INTRODUCE DATE (DIU)
NU
ADC COLECTEAZA ICU
AC TRIMITE DIU, ID, ADD, ICU SI CD2
PROCESEAZA DIU
DIU OK?
NU
POATE REINCERCA
DA
NU
DA
AC TRIMITE ID, ADD, SI CD2
ADF COLECTEAZA CD3
ADF TRIMITE CERERE DE EVALUARE
EVALUEAZA (DIU, ID, ADD, ICU, CD1, CD2, CD3, GRDA, BDFB)
DA
EVALUARE OK?
NU
FURNIZEAZA SERVICIUL / RESURSA
AFISEAZA
FURNIZEAZA INFORMATIE ALTERNATIVA
SFARSIT

Fig. 5

AGENTIA DE STAT PENTRU PROPRIETATEA INTELECTUALA A REPUBLICII MOLDOVA

RAPORT DE DOCUMENTARE

I. Datele de identificare a cererii

(21) Nr. depozit: s 2015 0017

(22) Data depozit: 2015.02.17

(71) Solicitant: **SOCIETATEA CU RĂSPUNDERE LIMITATĂ "SIGURANȚĂ TRANZACȚII", MD**

(54) **Titlul**: **Metodă de prevenire a infracțiunii la solicitarea prestării de servicii prin intermediul rețelei Internet**

II. Clasificarea obiectului invenției:

(51) **Int.Cl:** ***H04L 9/00*** (2006.01)
H04L 29/06 (2006.01)
H04K 1/00 (2006.01)

III. Colecții şi Baze de date de brevete cercetate (denumirea, termeni caracteristici, ecuații de căutare reprezentative)

MD - Intern « Documentare Invenții » (inclusiv cereri nepublicate; trunchiere automată stanga/dreapta): H04L, H04K, infracțiune, servicii, internet, autentificare, account, server, cookie, fișier

SU, EA, CIS (Eapatis): H04L*, H04K*, политика конфиденциальности, подозрительная активность, услуги, аутентификация, аккаунт, сервер, идентификация, провайдер

IV. Baze de date şi colecții de literatură nonbrevet cercetate

ru.wikipedia.org
www.google.ru

V. Documente considerate a fi relevante

Categoria*	Date de identificare ale documentelor citate si, unde este cazul, indicarea pasajelor pertinente	Numărul revendicării vizate
A, D, C	US7330871 B2 2008.02.12	1

*** categoriile speciale ale documentelor citate:**

A – document care defineşte stadiul anterior general	**T –** document publicat după data depozitului sau a priorității invocate, care nu aparține stadiului pertinent al tehnicii, dar care este citat pentru a pune în evidența principiul sau teoria pe care se bazează invenția
X – document de relevanță deosebită: invenția revendicată nu poate fu considerată nouă sau implicând activitate inventivă când documentul este luat în considerație de unul singur	**E –** document anterior dar publicat la data depozit național reglementar sau după aceasta dată
Y – document de relevanță deosebită: invenția revendicată nu poate fu considerată ca implicând activitate inventivă când documentul este asociat cu unul sau mai multe documente de aceiaşi categorie	**D** – document menționat în descrierea cererii de brevet

O - document referitor la o divulgare orală, un act de folosire, la o expoziție sau la orice alte mijloace de divulgare	**C** – document considerat ca cea mai apropiată soluție
	& – document, care face parte din aceeaşi familie de brevete
P - document publicat inainte de data de depozit, dar după data priorității invocate	**L** – document citat cu alte scopuri
Data finalizării documentării 2015.07.10	
Examinator GHIȚU Irina jr.	