ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 138145 A0**

(51) Int.Cl.
G06F 18/21 (2023.01),
G06F 18/214 (2023.01),
G06F 21/32 (2013.01),
G06N 3/08 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2023 00315**

(22) Data de depozit: **21/06/2023**

(41) Data publicării cererii:
30/04/2024 BOPI nr. **4/2024**

(71) Solicitant:
• **UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI**, *SPLAIUL INDEPENDENŢEI NR.313, SECTOR 6, BUCUREŞTI, B, RO;*
• **RESEARCH TECHNOLOGY S.R.L.**, *ŞOS.VIRTUŢII, NR.19D, ET.6, SECTOR 6, BUCUREŞTI, B, RO*

(72) Inventatori:
• **NEACSU TEODOR**, *SPLAIUL INDEPENDENŢEI, NR.313B, ET.4, AP.51, SECTOR 6, BUCUREŞTI, B, RO;*
• **RUSETI ŞTEFAN**, *STR.FABRICA DE GLUCOZĂ, NR.6-8, BL.9, SC.A, AP.15, SECTOR 2, BUCUREŞTI, B, RO;*
• **DASCALU MIHAI**, *STR.STOICA LUDESCU, NR.61, ET.1, AP.7, SECTOR 1, BUCUREŞTI, B, RO;*
• **BANICA COSMIN KARL**, *STR. BLANDEŞTI NR. 24C, SECTOR 4, BUCUREŞTI, B, RO*

(54) # SISTEM DE AUTENTIFICARE PRIN SECVENŢE DE TASTARE FOLOSIND PERECHI DE TASTE ŞI REŢELE NEURALE PROFUNDE

(57) **Rezumat:**

Invenţia se referă la o metodă de învăţare automată a reprezentărilor vectoriale ale perechilor de taste care încorporează informaţii despre utilizatorul care le-a generat, cu utilizare într-un sistem de autentificare. Metoda conform invenţiei cuprinde două faze, una de antrenare şi una de testare, în care faza de antrenare constă în trei etape:

- o etapă de corupere a secvenţelor de tastare pentru a seta configuraţia de învăţare auto-supervizată, etapă în care un dicţionar cu toate perechile de taste din setul de date al fiecărui utilizator este folosit pentru a înlocui caracteristicile temporale pentru elementele selectate din secvenţe,
- o etapă de construire a secvenţelor de intrare, în care o secvenţă este asamblată prin ataşarea reprezentării utilizatorului de secvenţa de elemente de tastare construite prin concatenarea reprezentărilor tastelor şi a caracteristicilor temporale, şi
- o etapă de antrenare în care reţeaua discriminatoare învaţă să diferenţieze între perechi autentice şi perechi corupte, etapă în care se foloseşte un model care generează reprezentări contextualizate şi le foloseşte pentru a clasifica elementele de tastare în originale şi corupte, iar faza de testare vizează un protocol de autentificare bazat pe numărul de elemente de tastare clasificate ca originale, ale utilizatorului vizat.

Revendicări: 5
Figuri: 4

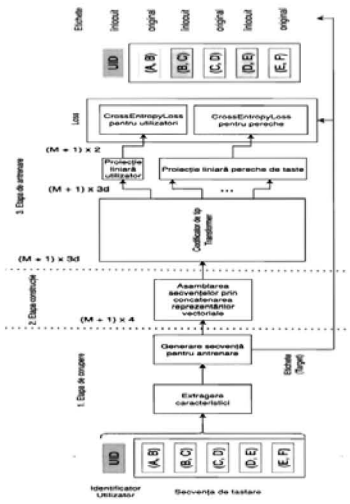

Fig. 1

Cu începere de la data publicării cererii de brevet, cererea asigură, în mod provizoriu, solicitantului, protecţia conferită potrivit dispoziţiilor art.32 din Legea nr.64/1991, cu excepţia cazurilor în care cererea de brevet de invenţie a fost respinsă, retrasă sau considerată ca fiind retrasă. Întinderea protecţiei conferite de cererea de brevet de invenţie este determinată de revendicările conţinute în cererea publicată în conformitate cu art.23 alin.(1) - (3).

RO 138145 A0

54

I. DESCRIERE

OFICIUL DE STAT PENTRU INVENȚII ȘI MĂRCI
Cerere de brevet de invenție
Nr. a 2023 00 315
Data depozit 21 -06- 2023

Titlu

„Sistem de Autentificare prin Secvențe de Tastare folosind Perechi de Taste și Rețele Neurale Profunde"

Prezentarea domeniului de aplicare

Invenția se referă la o metodă de învățare automată a reprezentărilor vectoriale pentru fiecare utilizator dintr-un sistem de autentificare. Reprezentările latente codifică diferitele moduri de tastare ale utilizatorilor, iar obiectivul final presupune autentificarea utilizatorilor folosind reprezentarea vectorială și un număr redus de taste. Domeniul de aplicare al metodei este vast, aceasta contribuind la nevoia tot mai mare de metode de autentificare sigure în diverse industrii. Autentificarea biometrică are mai multe avantaje față de metodele tradiționale de autentificare, cum ar fi parolele sau codurile PIN, deoarece caracteristicile biometrice sunt unice pentru fiecare individ și nu pot fi ușor replicate sau furate. Semnătura biometrică prin tastare este un tip de autentificare biometrică comportamentală care utilizează tiparele unice de tastare ale indivizilor pentru a le verifica identitățile. Biometria apăsării tastelor are mai multe avantaje față de alte metode de autentificare biometrică, cum ar fi recunoașterea facială sau a amprentei, deoarece nu necesită hardware suplimentar și poate fi implementată pe aproape orice dispozitiv cu tastatură.

Biometria apăsării tastelor are multiple cazuri de utilizare în industrii precum domeniul bancar, comerț electronic și asistență medicală, unde poate fi utilizată pentru a autentifica utilizatorii într-un mod sigur și convenabil.

Stadiul tehnicii

Brevetul EP3557458A1 (https://patents.google.com/patent/EP3557458A1) propune o metodă de generare a unor șiruri de caractere care urmează să fie afișate unui utilizator la un terminal în vederea autentificării utilizatorului prin analiza comportamentului acestuia la tastarea șirurilor de caractere pe tastele unei tastaturi. Dezavantajul acestei invenții este că secvența introdusă de către utilizator este prestabilită, acest lucru determinând imposibilitatea autentificării prin introducerea de text liber.

Brevetul US10970573B2 (https://patents.google.com/patent/US10970573B2) propune o metodă de analiză bazată pe GMM (Gaussian Mixture Model) a datelor de apăsare a tastelor preprocesate sub formă de perechi de taste. Pentru fiecare pereche de taste sunt colectate date și, folosind aceste date, sunt construiți vectori caracteristici grupați conform perechilor. Dezavantajul acestei invenții este enunțat de către autorii brevetului și presupune inferioritatea din punctul de vedere al performanței modelului de tip Gaussian Mixture Model care a fost selectat pentru viteza computațională și posibilitatea rulării pe dispozitive cu resurse limitate.

52

TypeNet [*Alejandro Acien, Aythami Morales, John V. Monaco, Ruben Vera-Rodriguez & Julian Fierrez (2021) TypeNet: Deep Learning Keystroke Biometrics,* https://arxiv.org/abs/2101.05570] foloseşte reţele neurale recurente cu celule de tip LSTM [*Hochreiter, Sepp & Schmidhuber, Jürgen. (1997). Long Short-term Memory. Neural computation. 9 1735-80,* https://www.researchgate.net/publication/13853244_Long_Short-term_Memory] pentru construirea de şabloane pentru fiecare secvenţă din setul de date de antrenare. Folosind funcţii de optimizare precum ContrastiveLoss sau TripletLoss, fiecare utilizator are proiectate şabloanele de tastare într-un spaţiu vectorial. Decizia de autentificare este determinată calculând pentru o secvenţă nouă distanţa euclidiană medie dintre reprezentarea calculată şi o medie a reprezentărilor produse din setul de antrenare pentru fiecare utilizator. Decizia de autentificare este luată folosind un prag limită pentru această distanţă. O limitare a acestei metode o reprezintă folosirea arhitecturii LSTM; această arhitectură este inferioară arhitecturilor de tip Transformer vizată de prezentul brevet [*Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Paper presented at the 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA*], rezultând în reprezentări latente deficitare ale secvenţelor.

O abordare similară pentru generarea de şabloane de tastare este reţeaua TypeFormer [*Giuseppe Stragapede, Paula Delgado-Santos, Ruben Tolosana, Ruben Vera-Rodriguez, Richard Guest, Aythami Morales, (2022), TypeFormer: Transformers for Mobile Keystroke Biometrics,*

https://arxiv.org/abs/2212.13075] care foloseşte o arhitectura modificată de Gated Transformer Network [*Minghao Liu, Shengqi Ren, Siyuan Ma, Jiahui Jiao, Yizhou Chen, Zhiguang Wang, Wei Song, (2021), Gated Transformer Networks for Multivariate Time Series Classification, https://arxiv.org/abs/2103.14438*]. TypeFormer generează şabloane de tastare agregând 2 tipuri de reprezentări vectoriale: una generată la nivel de secvenţă, iar cealaltă generată la nivel de caracteristică. Dezavantajul acestei metode este că aceasta generează reprezentări vectoriale pentru secvenţe independent de utilizatori, scopul principal fiind delimitarea secvenţelor care aparţin utilizatorilor diferiţi într-un spaţiul latent al reprezentărilor.

Prezentarea sintetică a invenţiei

Problema tehnică pe care invenţia îşi propune să o rezolve vizează limitările metodelor actuale de autentificare biometrică prin secvenţe de tastare care folosesc întregile secvenţe pentru a genera reprezentări vectoriale fără să includă informaţii despre utilizatori. Metoda propusă primeşte ca intrare o secvenţă care are ca prim element reprezentarea vectorială a utilizatorului urmată de elemente care reprezintă perechile de tastare care includ caracteristici temporale. O arhitectură de codificare de tipul Transformer (eng. "Transformer Encoder") este folosită pentru generarea reprezentărilor contextualizate ale perechilor de taste, urmată de o proiecţie liniară pentru elementele corespunzătoare perechilor. Secvenţele folosite pentru antrenare sunt generate

pentru o antrenare auto-supervizată (eng. "self-supervised") care include atât perechi autentice de la o colecție de utilizatori, cât și perechi corupte.

Un beneficiu major al acestei metode presupune folosirea unor reprezentări latente ale utilizatorilor pentru a diferenția perechile de taste autentice de cele corupte. Folosirea acestei metode elimină problema lungimii secvențelor de antrenare a modelelor, acesta reprezentând un element care influențează puternic performanța celorlalte metode. Metoda propusă introduce un protocol nou de autentificare pe baza perechilor de taste.

Avantaje

Metoda conform invenției prezintă următoarele avantaje:

- Generarea reprezentărilor vectoriale pentru fiecare tastă.
- Generarea reprezentărilor vectoriale pentru perechile de taste combinate prin concatenarea reprezentărilor pentru fiecare tastă cu o proiecție a caracteristicilor temporale ale perechii de taste.
- Generarea reprezentărilor vectoriale pentru fiecare utilizator folosite pentru contextualizarea reprezentărilor perechilor de taste.

- Discriminarea perechilor de taste pe baza reprezentării utilizatorului are la bază o rețea de codificare de tip Transformer care îmbunătățește atât reprezentările vectoriale ale tastelor, cât şi ale utilizatorilor.

- Protocolul de autentificare este bazat pe numărul de perechi de taste clasificate drept autentice coroborate cu reprezentarea utilizatorului şi nu pe o distanță euclidiană.

Prezentarea figurilor

În continuare, invenția va fi descrisă în detaliu. Figura 1 prezintă întreaga schemă de antrenare de tip învățare auto-supervizată (eng. „Self Supervised Learning") pornind de la datele brute până la obiectivul necesar antrenării rețelei neurale discriminator.

Figura 2 prezintă metoda de extragere a caracteristicilor temporale reprezentate de diferențe temporale între evenimentele dintre 2 taste consecutive. Datele brute sunt reprezentate de secvențe în care fiecare element are 3 caracteristici: tasta cu care s-a interacționat, tipul de eveniment şi momentul de timp al evenimentului. Un element din secvența procesată este determinat de cele 4 caracteristici temporale şi cele 2 taste.

Figura 3 introduce metoda de corupere a secvențelor de tastare care înlocuiește aleatoriu caracteristici temporale ale perechilor de taste din secvență. Prima decizie de luat este dacă secvența curentă este coruptă sau nu. Dacă secvența curenta este coruptă, următorul pas presupune

alegerea aleatorie a perechilor de înlocuit. Ulterior, caracteristicile temporale sunt înlocuite cu altele alese aleatoriu de la alți utilizatori.

Figura 4 prezintă metoda de construire a secvenței dată la intrarea rețelei discriminator. Secvența este compusă din reprezentarea utilizatorului ca prim element, urmată de reprezentările perechilor de taste.

Descrierea detaliată a invenției

Metoda propusă presupune o fază de antrenare în care o rețea neurală discriminator învață reprezentări vectoriale latente pentru taste și utilizatori pentru diferențierea perechilor autentice de cele ce vor fi corupte urmată de o fază de testare în care este introdus un nou protocol de autentificare bazat pe predicții la nivel de perechi de taste. Faza de antrenare cuprinde trei etape: a) o etapă de corupere în care sunt selectate și înlocuite caracteristicile perechilor de taste, b) o etapă de construcție în care reprezentările vectoriale ale perechilor de taste sunt asamblate și reprezentarea utilizatorilor este atașată, și c) o etapă de antrenare în care rețeaua neurală învață să discrimineze perechile autentice.

În faza de antrenare presupunem că metoda de clasificare a perechilor de taste are la dispoziție următoarele componente:

- Un set de secvențe de tastare și identificatorii utilizatorilor respectivi.

47

- Un tabel de reprezentări vectoriale pentru taste.
- Un tabel de reprezentări vectoriale pentru utilizatori.
- Un dicționar cu perechile de taste prezente în secvențele de antrenare ale utilizatorilor. Pentru fiecare pereche de taste sunt menținute caracteristicile temporale pentru fiecare apariție și utilizatorul de la care provine respectiva pereche.
- Metodă de corupere a secvențelor date la intrare pentru a genera exemple negative.
- Metodă de generare a secvențelor de intrare prin concatenarea subreprezentărilor vectoriale ale componentelor (taste și caracteristici temporale).
- O rețea discriminator care diferențiază între perechile autentice și perechile corupte folosind atât secvența, cât și reprezentarea latentă a utilizatorilor.

Datele de intrare pentru această metodă sunt reprezentare de secvențe de tastare în care fiecare element este reprezentat de o tasta cu 3 caracteristici aferente: codul tastei, tipul de eveniment (apăsare/eliberare) și momentul de timp. Fiecare secvență este transformată împerechind tastele și extrăgând caracteristicile temporale definite de diferențele următoare de timp:

- HL (eng. „Hold Latency") – diferența de timp dintre apăsarea și eliberarea aceleiași taste.
- IL (eng. „Inter-Key Latency") – diferența de timp dintre eliberarea unei taste și apăsarea următoarei taste.
- PL (eng. „Press Latency") – diferența de timp dintre două apăsări de taste consecutive.

46

- RL (eng. „Release Latency") – diferența de timp dintre două eliberări de taste consecutive.

Fiecare element dintr-o secvență de tastare are următoarele caracteristici: 4 caracteristici temporale și 2 coduri aferente primei și celei de-a doua taste. Pentru fiecare tastă este salvat câte un identificator care determină reprezentarea vectorială în tabelul de reprezentări ale tastelor. După antrenarea modulului, reprezentările latente ale tastelor vor incorpora informații referitoare la poziția relativă tastelor pe diferitele tipuri de tastaturi (spre exemplu, qwerty, qwertz sau azerty). Fiecare utilizator din setul de date are asociat un identificator care determină poziția sa în tabelul de reprezentări vectoriale.

Pentru învățarea reprezentărilor latente ale tastelor și ale utilizatorilor este aplicată o metodă de antrenare auto-supervizată similară cu cea folosită în ELECTRA [*Clark, K., Luong, M., Le, Q. V., & Manning, C. D. (2020). ELECTRA: pre-training text encoders as discriminators rather than generators. In International Conference on Learning Representations, Addis Ababa, Ethiopia*]. Scopul rețelei discriminator este să diferențieze, utilizând reprezentarea latentă a utilizatorului, perechile de taste autentice de perechile de taste corupte folosind totodată și caracteristicile temporale ale acestora. Secvențele de tastare pentru antrenare au probabilitatea de a fi corupte p_{user}. Dacă secvența este coruptă, sunt alese $\max(k_{\text{corupt}} * \text{lungime(secvență)}, 1)$ perechi de taste care urmează să fie corupte, unde k_{corupt} este procentul maxim de corupere a unei secvențe. Această valoare este setată experimental la diverse valori pentru a determina procentul optim de corupere. Procesul de corupere constă în înlocuirea caracteristicilor temporale ale perechilor selectate cu alte

valori corespunzătoare aceleiaşi perechi date de la alt utilizator. Pentru această parte este necesar dicţionarul de perechi prezentat în Figura 3 care conţine pentru fiecare utilizator perechile de taste din setul de antrenare şi caracteristicile temporale corespunzătoare. Pe lângă secvenţa coruptă, această etapă generează şi un vector cu etichete pentru perechi (original/înlocuit). Prin această corupere a secvenţelor, la antrenare sunt disponibile atât perechi de taste pozitive cât şi perechi de taste negative, ambele benefice pentru antrenarea reţelei neurale discriminator.

O secvenţă de tastare pentru antrenare este compusă din identificatorul utilizatorului urmat de M elemente (numărul maxim de perechi dintr-o secvenţă) conţinând perechile de taste şi cele 4 caracteristici temporale specifice fiecărei perechi. Pentru a genera reprezentarea utilizatorului, identificatorul său va fi folosit pentru extragerea reprezentării de dimensiune $3 \times d$. Pentru construirea reprezentărilor pentru perechile de taste sunt aplicaţi următorii paşi:

- trecerea vectorului cu caracteristici temporale printr-o proiecţie liniară pentru a ajunge în dimensiunea d urmată de o normalizare,
- trecerea tastelor K_1 şi K_2 prin tabelul de reprezentări pentru extragerea reprezentărilor acestora (reprezentările vectoriale au dimensiune d) şi
- concatenarea celor 3 vectori pentru a genera reprezentarea vectorială a unui element (reprezentarea finală are dimensiunea $3 \times d$, aceeaşi cu cea a utilizatorului).

Secvența de intrare pentru antrenarea rețelei de codificare de tip Transformer folosită pentru generarea reprezentărilor contextualizate are dimensiunea $(M + 1) \times 3d$, iar secvența de ieșire are aceeași dimensiune. Reprezentările perechilor de taste sunt trecute printr-un strat linear, iar ieșirea este reprezentată de o secvență de dimensiune $M \times 2$ (2 reprezentând numărul de clase – original/înlocuit). Obiectivul rețelei presupune determinarea perechilor de taste care nu sunt specifice utilizatorilor (perechile de taste corupte). Funcția de eroare folosită este CrossEntropyLoss [*Zhang, Zhilu, and Mert Sabuncu. "Generalized cross entropy loss for training deep neural networks with noisy labels." Advances in neural information processing systems 31 (2018)*], aplicată pe ieșirea rețelei și pe vectorul de etichete.

După antrenarea rețelei care discriminează perechile corupte de cele originale, metoda propusă introduce un protocol de autentificare care are la bază identificarea de secvențe care nu aparțin utilizatorului care folosește în mod normal echipamentul. Fiecare secvență de tastare are asociată un scor determinat de numărul de perechi de taste care au fost clasificate drept autentice, iar fiecare utilizator are o valoare de prag care determină dacă utilizatorul este autentificat sau nu. Evaluarea performanței consideră drept metrică Equal Error Rate (EER) [*Bours, Patrick, and Soumik Mondal. "Performance evaluation of continuous authentication systems." Iet Biometrics 4, no. 4 (2015)*] determinată de intersecția dintre False Acceptance Rate (FAR) și False Rejection Rate (FRR).

II. REVENDICĂRI

1. Metoda de autentificare a utilizatorilor bazată pe reprezentările vectoriale latente ale perechilor de taste şi ale utilizatorilor, cuprinzând o fază de antrenare şi o fază de testare, **caracterizată prin aceea că,** în *faza de antrenare*, se aplică o metodă de învăţare de tip auto-supervizată pe secvenţele preprocesate care presupune 3 etape: etapa de corupere a secvenţelor de tastare prin înlocuirea caracteristicilor temporale, o etapă de construcţie în care sunt asamblate secvenţele de intrare şi o etapă de antrenare în care reţeaua discriminator învaţă să diferenţiaze perechile de taste autentice de cele corupte.

2. Metoda de calcul **conform revendicării 1, caracterizată prin aceea că**, generarea secvenţelor de antrenare cuprinde o primă etapă care presupune selectarea unor perechi de taste care urmează să fie corupte, urmată de o etapă de înlocuire a elementelor selectate cu un alt set specific aceleiaşi perechi, dar provenind de la alt utilizator, utilizând un dicţionar de perechi de taste în care sunt reţinute pentru fiecare utilizator perechile de taste din setul de antrenare şi caracteristicile temporale pentru fiecare apariţie.

3. Metoda de calcul **conform revendicării 1, caracterizată prin aceea că**, etapa de construcţie a secvenţelor de tastare presupune caracterizarea fiecărei perechi de taste folosind 4 valori care reprezintă diferenţe de timp între evenimentele de apăsare şi eliberare ale celor 2 taste considerate, iar vectorul rezultat este proiectat folosind o transformare

liniară într-un vector de dimensiune prestabilită care este concatenat cu reprezentările vectoriale latente aferente celor 2 taste, de aceeaşi dimensionalitate.

4. Metoda de calcul **conform revendicării 1, caracterizată prin aceea că**, etapa de antrenare utilizează măşti vectoriale care conţin indicii elementelor corupte şi presupune antrenarea reţelei neurale discriminator bazată pe arhitectura *Transformer* pentru generarea reprezentărilor contextualizate ale secvenţei perechilor de tastare care includ informaţiile utilizatorilor, folosite în combinaţie cu transformări liniare, pentru diferenţierea între perechi originale şi perechi corupte.

5. Metoda de calcul **conform revendicării 1, caracterizată prin aceea că,** în *faza de testare* a reţelei neurale discriminator este introdus un protocol de autentificare bazat pe numărul de perechi de taste clasificate ca fiind originale; valoarea de prag specifică sistemelor de autentificare este bazată pe acest scor, decizia de autentificare fiind luată doar dacă scorul secvenţei de intrare este mai mare decât scorul de prag specific fiecărui utilizator.

41

III. DESENE EXPLICATIVE

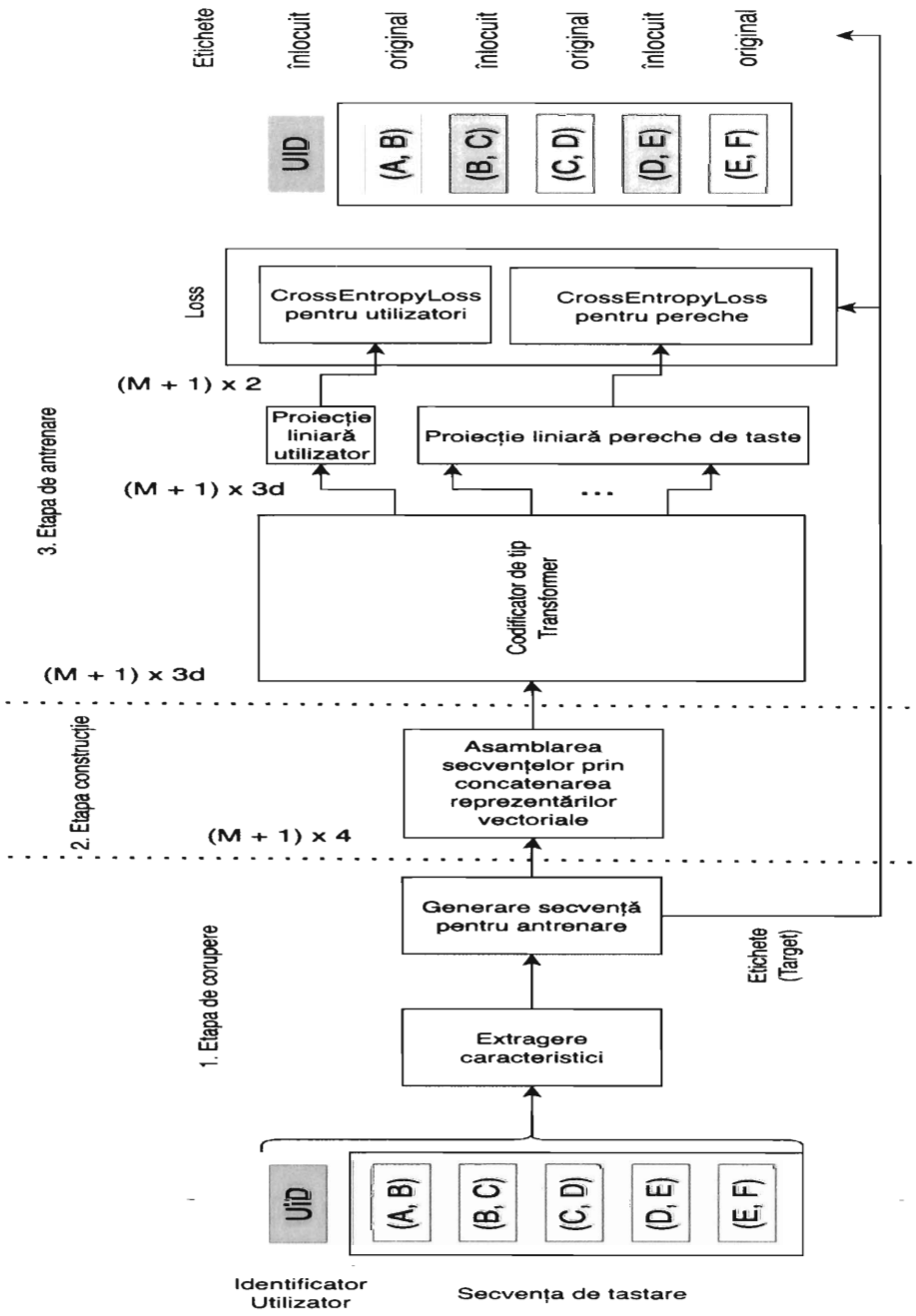

Fig. 1 Antrenarea modelului folosind învățare auto-supervizată

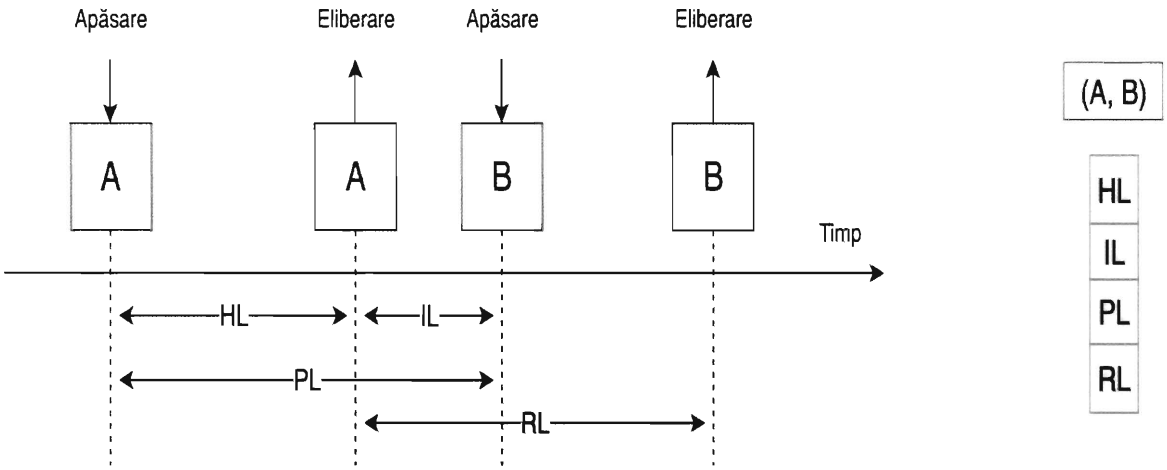

Fig. 2 Extragerea caracteristicilor temporale

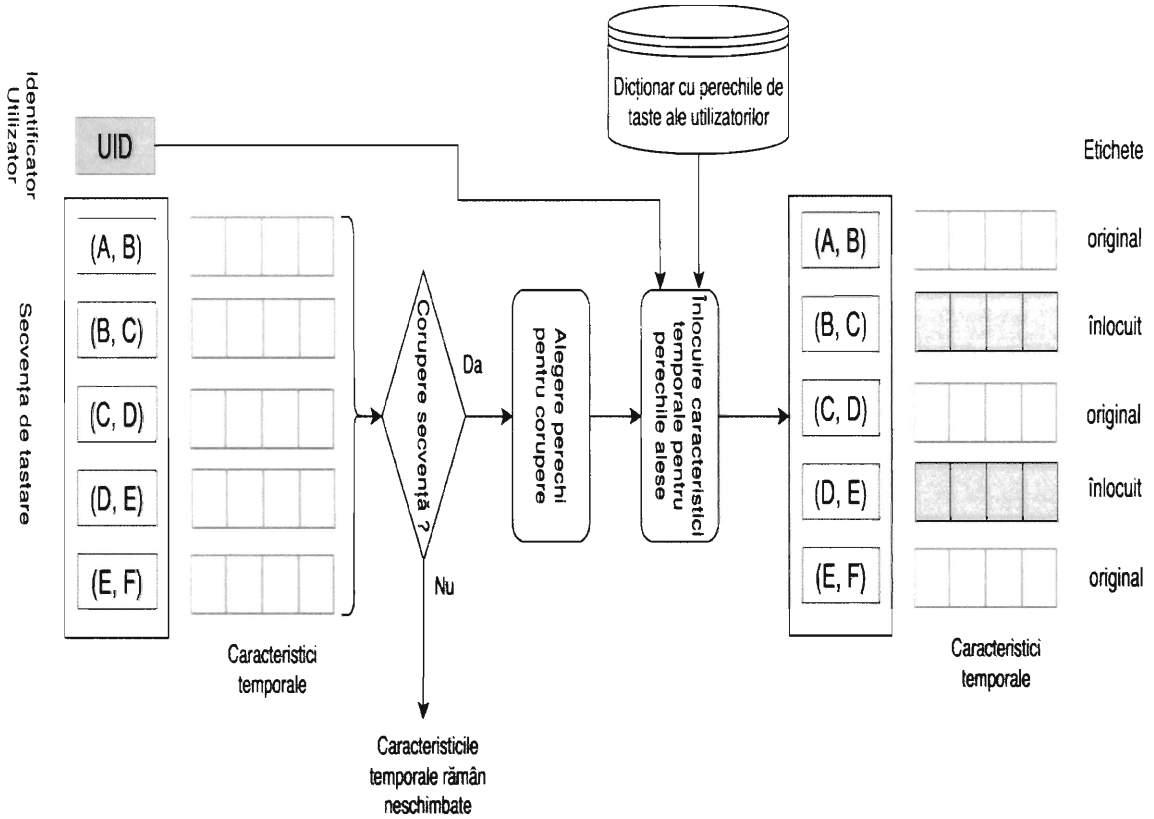

Fig. 3 Coruperea secvențelor de antrenare prin înlocuirea caracteristicilor temporal

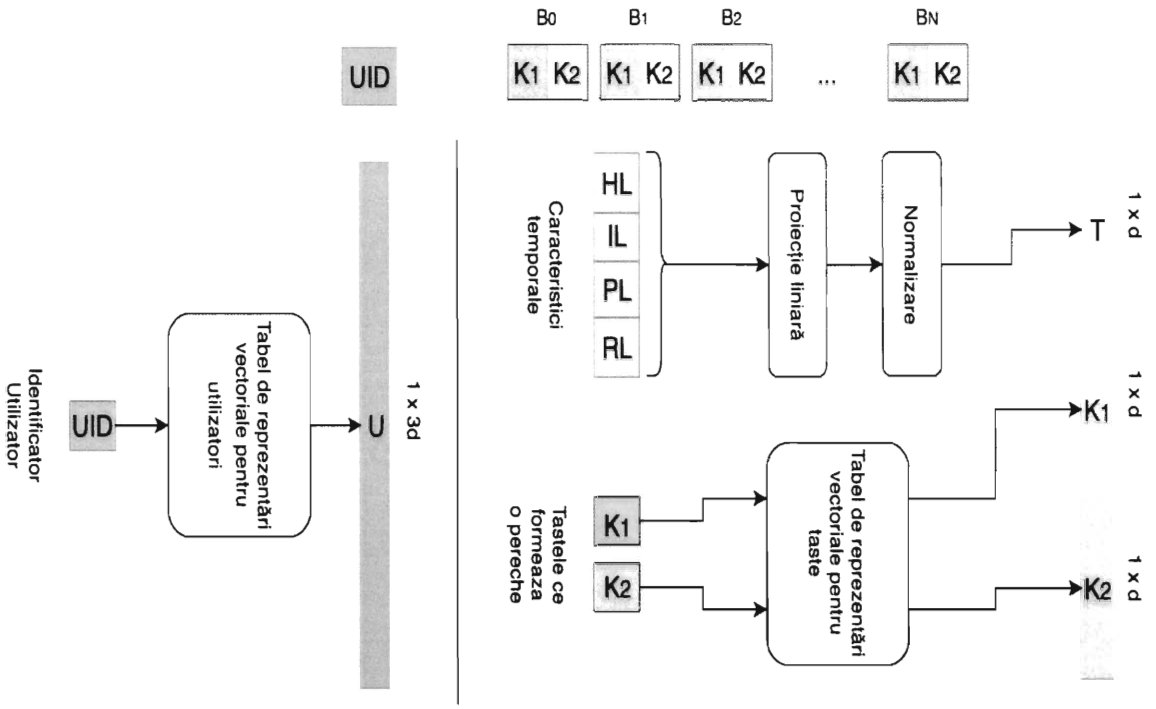

Fig. 4 Construcția secvenței de intrare pentru antrenarea modelului