ACHIZIŢII DE DATE PENTRU AUTENTIFICARE

Ion Ivan **Adrian Pocovnicu** **Andrei Pătraşcu** **Daniel Milodin**

Academia de Studii Economice, Bucureşti

Rezumat: Se defineşte conceptul de autentificare în sisteme distribuite. Sunt prezentate modalităţi de achiziţie de date sub formă de şiruri de caractere, date biometrice, carduri.
Este proiectat un sistem de contabilitate distribuit pentru a aplica moduri diferite de achiziţii de date.

Cuvinte cheie: autentificare, achiziţie de date, date biometrice, parole, carduri

1. Autentificarea - cerinţă în sistemele distribuite

Sistemele distribuite presupun:

- existenţa mai multor calculatoare conectate în reţea;
- utilizarea de aplicaţii care să fie accesate din mai multe staţii de lucru;
- lucrul on-line;
- acces la resursele internet sau la alte reţele de calculatoare;
- partajarea resurselor;
- existenţa unei diversităţi de persoane care doresc să soluţioneze probleme folosind aceste aplicaţii;
- realizarea funcţiei de mentenanţă de către persoane aflate, de asemenea, în diferite locaţii geografice;
- operaţii de prelucrare pe diferite niveluri de acces; informarea de către toţi, consultarea de către cei interesaţi direct, adăugarea de către operatori în sens larg, modificări şi ştergeri temporare de către administratori.

Autentificarea este operaţia prin care se verifică dacă există concordanţă între elementele unei liste numită de referinţă cu elementele generate la un terminal.

Autentificarea în sisteme distribuite presupune existenţa unei clasificări a utilizatorilor care au acces în sistemul distribuit. O ierarhie simplă presupune existenţa unui grup de administratori şi a unui grup de utilizatori generici. Clasificarea utilizatorilor se poate face atât din punct de vedere al operaţiilor pe care le pot efectua, cât şi din punct de vedere al informaţiei care poate fi accesată.

Se consideră aplicaţia **A** destinată soluţionării unei probleme din clasa **P**. Există un număr de **N** persoane care asigură gestiunea aplicaţiei şi un număr **M** de persoane care utilizează aplicaţia pentru a soluţiona probleme concrete din clasa **P**, folosind date proprii.

Lista administratorilor conţine un număr de N perechi (a_i,p_i) unde a_i sunt nume de administratori şi p_i sunt parole, de fapt şiruri de caractere. Lista utilizatorilor conţine M perechi (a_j,p_j) unde a_j sunt nume de utilizatori şi p_j parole date tot sub formă de şiruri de caractere.

A autentifica un administrator înseamnă a compara şirurile furnizate de o persoană cu perechile din lista de administrare. Numai în cazul de egalitate perfectă atât a numelui de administrator, cât şi a parolei se permite accesul pentru a se efectua operaţii precum:

- modificarea câmpurilor în baza de date;
- modificarea listelor de parole la utilizatori;
- modificarea structurii interfeţelor;
- modificarea secvenţelor de program;
- instalarea de noi proceduri de prelucrare;
- instalarea de noi versiuni.

Procesului de autentificare a administratorului definit prin perechea (a_k,p_k) îi corespunde diagrama:

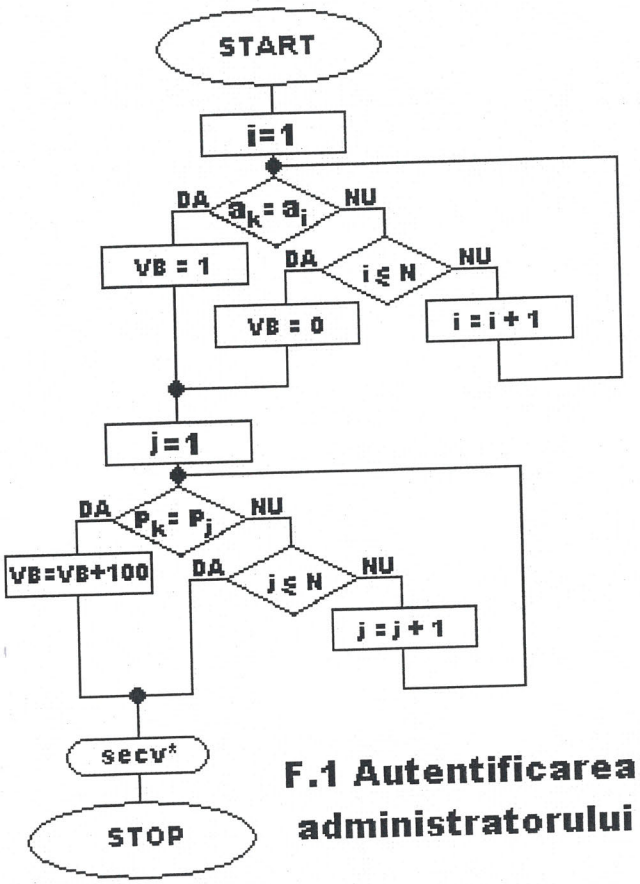

Figura 1. Autentificarea administratorului

unde:

i – contor folosit pentru parcurgerea utilizatorilor cu drept de autentificare;

a_i – utilizatorul corespunzător indicelui i;

N – numărul total de utilizatori înregistrați;

VB – variabilă ce poate lua valorile 0, 1, 100 sau 101 după cum urmează:

- dacă atât utilizatorul, cât şi parola sunt greşite atunci VB este 0;
- dacă doar parola este greşită atunci VB este 1;
- dacă utilizatorul este greşit, dar există parola, atunci VB este 100;
- dacă autentificarea este reuşită atunci VB este 101.

j – contor folosit pentru parcurgerea parolelor înregistrate;

p_i – parola corespunzătoare indicelui i.

Secvenței **secv*** îi pot corespunde două scheme, în funcție de metoda dorită de autentificare. Prima variantă a metodei figura 2a presupune afişarea numai a două mesaje, în funcție de situație: *autentificare reuşită* ori *utilizator sau parolă incorectă.* Avantajul acestei variante este reprezentat de un grad de siguranță crescut, deoarece cel ce se identifică nu cunoaşte cu exactitate ce parte a autentificării a fost incorectă. Prin a doua variantă figura 2b i se furnizează persoanei ce se identifică date exacte despre ce a greşit: utilizatorul, parola sau ambele.

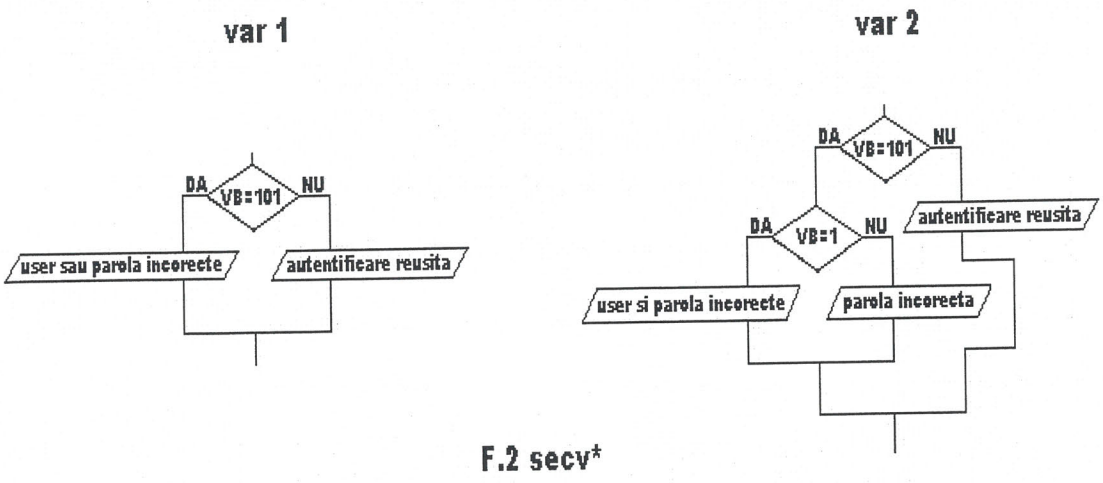

Figura 2. secv*

Autentificarea prin şiruri de caractere este utilizată, în prezent, prin sistemele de parole şi de carduri. A autentifica utilizatorii înseamnă a compara şirurile de caractere introduse de o persoană care reprezintă numele utilizatorului şi parola, cu şirurile de caractere existente în lista de **M** perechi şi numai în caz de egalitate utilizatorul autentificat are dreptul să efectueze operaţiile definite pentru el, precum:

- consultarea bazei de date;
- definirea de probleme de rezolvat;
- crearea unui fişier utilizator cu datele problemei pe care o rezolvă;
- selectarea de opţiuni de prelucrare;
- definirea de opţiuni de afişare rezultate;
- salvarea de probleme şi de date de intrare şi rezultate;
- integrarea de secvenţe de prelucrare proprii.

Acest mod de autentificare este clasic.

Se definesc mai multe liste de parole, depinzând de numărul de categorii de acces la resurse cu care se lucrează.

Autentificarea biometrică presupune folosirea trăsăturilor fiziologice şi comportamentale proprii unei persoane în scopul identificării acesteia ca administrator sau utilizator al unei baze de date distribuite. În funcţie de caracteristicile folosite, poate fi autentificare biometrică bazată pe amprentă, iris, retină, portret uman, geometria palmei, semnătură sau voce. Primele cinci din această enumerare sunt trăsături fizice şi, în consecinţă, destul de greu alterabile, pe când ultimele două sunt mult mai uşor influenţate de caracterul nostru uman.

Autentificarea biometrică funcţionează în mare măsură ca şi cea clasică-pe bază de parolă-în sensul că datele sunt captate, codificate folosind diferiţi algoritmi, şi stocate pe un suport fizic. Identificarea propriu-zisă se face comparând datele preluate de la persoana ce încearcă să acceseze baza de date cu datele existente pe suportul fizic.

Dar când şi cum a fost introdusă identificarea pe baza trăsăturilor individuale proprii unei persoane? Totul a pornit în perioada anilor 1890-1900, când a fost introdus un sistem nou de identificare a criminalilor. Sistemul creat de antropologul Alphonse Bertillon se baza, în esenţă, pe faptul că scheletul uman, respectiv oasele adulte, după vârsta de 20 de ani, au aceeaşi lungime pe parcursul vieţii. El presupunea măsurarea unor trăsături ca dimensiunile capului sau lungimea diverselor oase şi compararea lor cu măsurătorile făcute anterior. Cu toate că procesul de înregistrare a datelor, măsurarea propriu-zisă a persoanei, dura între 20 şi 60 de minute; sistemul, în ansamblu, era destul de rapid şi eficient pentru vremurile respective.

În anul 1903 însă, la închisoarea Fort Leavenworth, au fost înregistrate pentru prima dată două seturi de date identice pentru persoane diferite, astfel că s-a hotărât renunţarea la acest sistem şi trecerea la identificarea pe bază de amprentă.

2. Autentificarea folosind amprenta digitală

Se foloseşte în investigaţiile criminalistice de mai bine de 100 de ani. Îşi are originile în China secolului al XIV-lea, când părinţii foloseau această metodă pentru a-şi deosebi copiii de cei ai altora.

În a doua jumătate a secolului al XIX-lea, au fost create două metode de catalogare şi identificare a semnelor ce compun o amprentă. Prima metodă a fost introdusă de Francis Galton în 1892 şi perfecţionată de către Richard Edward Henry, ce activa în cadrul Scotland Yard, iar cea de-a doua a fost propusă în anul 1891 de Juan Vucetich. Ambele metode sunt folosite şi în ziua de astăzi.

Autentificarea folosind amprenta digitală a devenit realitate o dată cu dezvoltarea senzorilor de presiune şi ultrasunete. Metoda se referă la a compara două amprente umane. Amprenta este una dintre modalităţile biometrice de a identifica un individ.

Analiza amprentelor necesită compararea câtorva caracteristici din modelul imprimat. În analiza amprentelor se urmăreşte atât tiparul pe care îl urmăresc striaţiile de pe deget, cât şi elementele unice, care apar în model.

Striaţiile amprentei sunt distribuite sub forma a trei tipare:

- arc - striaţiile încep dintr-o parte a degetului, formează un arc în centrul degetului şi se termină în cealaltă parte a degetului;
- buclă - striaţiile încep dintr-o parte a degetului, formează o buclă în centrul degetului şi au tendinţa să iasă pe aceeaşi parte a degetului;
- spirală - striaţiile formează o spirală în centrul degetului; interesant este că s-a descoperit ştiinţific faptul că este tipic ca membrii aceleaşi familii să moştenească acelaşi tipar al striaţiilor.



Figura 3. Arc



Figura 4. Buclă



Figura 5. Spirală

Elementele unice în interiorul amprentei sunt terminaţiile striaţiilor, bifurcarea striaţiilor precum şi striaţiile foarte scurte numite puncte.

Pentru a capta imaginea digitală a amprentei, se folosesc senzori. Imaginea captată este procesată digital pentru a crea un şablon, colecţie de caracteristici, care este înregistrat şi utilizat pentru comparaţii.

Cei mai des utilizaţi senzori sunt: optic, ultrasunete şi electromagnetici. Senzorii optici presupun captarea imaginii folosind lumina vizibilă. Degetul se aşează pe o suprafaţă transparentă. Dedesubt se află o sursă de lumină care luminează degetul. Lumina reflectată este captată sub formă de imagine. Principalele dezavantaje ale acestei metode de captare a imaginii le reprezintă dependenţa de calitatea suprafeţei pe care este aşezat degetul, precum şi dependenţa de condiţia pielii de pe deget, care nu trebuie să fie murdară sau erodată.

Ultrasunetele folosesc aceleaşi principii ca ultrasonografia în medicină, pentru a crea o imagine vizuală a amprentei. Spre deosebire de senzorii optici, senzorii pe bază de ultrasunete folosesc sunete de înaltă frecvenţă pentru a străpunge epiderma. Deoarece derma prezintă aceleaşi caracteristici ca epiderma, undele sonore reflectate de dermă pot fi utilizate pentru a crea o imagine a amprentei. Aceasta elimină necesitatea ca pielea de pe deget să fie curată şi nevătămată şi ca suprafaţa pe care se expune degetul să fie curată.

Algoritmii utilizaţi pentru a compara două amprente se încadrează în două categorii: algoritmi care se bazează pe analiza tiparului striaţiilor care formează amprenta şi algoritmi care se bazează pe analiza caracteristicilor unice din interiorul unei amprente.

Algoritmii care se bazează pe analiza tiparului striațiilor ce formează amprenta (arc, buclă, spirală) compară mprenta candidat cu şabloanele amprentelor memorate anterior. În acest caz, imaginile trebuie să fie orientate n aceeaşi direcţie. În acest tip de algoritm, şabloanele includ tipul tiparului, dimensiunea şi orientarea. maginea este comparată grafic cu celelalte şabloane existente şi se determină gradul de asemănare.

Algoritmii care se bazează pe analiza detaliilor unice din interiorul unei amprente (terminații, ɔifurcații, puncte) compară aceste detalii extrase dintr-un şablon cu cele extrase din amprenta candidat.

Avantajele acestei tehnologii de autentificare sunt spațiul mic de stocare, necesar informațiilor ɔbținute prin digitizarea amprentei, şi probabilitatea foarte mică, estimată ca fiind de 1 la 64 de miliarde, de a obține două seturi de date identice.

Pentru a securiza autentificarea folosind amprenta digitală, multe dintre sistemele existente astăzi verifică şi circulația sângelui prin deget sau dispunerea corectă a striațiilor ce formează amprenta spre marginea degetului. Cele mai multe sisteme nu au practic o imagine a amprentei, ci doar un set de date, obținut prin codificarea pe baza unui algoritm folosit pentru comparări ulterioare, de asemenea, din motive de securitate. În ciuda celor prezentate mai sus, există încă persoane ce se tem să nu le fie furate amprentele sau care pur şi simplu nu au încredere în autentificarea prin amprentă digitală.

3. Autentificarea folosind irisul ochiului şi retina

A început o dată cu dezvoltarea imaginilor digitale de înaltă precizie.

Istoria acestui tip de autentificare porneşte de la oftalmologul Frank Burch care, în anul 1936, a avut pentru prima dată ideea de a folosi irisul pentru a identifica o persoană. Mai mult de o jumătate de secol a fost necesar să treacă pentru ca metoda să fie patentată de doi colegi de breaslă ai lui Burch şi anume doctorii Leonard Flom şi Aran Safir, în anul 1987. După patentare, cei doi au apelat la serviciile doctorului John Daugman, matematician de profesie şi profesor la Universitatea Harvard, pentru a crea un algoritm de codificare a imaginii. În anul 1994, algoritmii erau deja gata, iar în prezent drepturile exclusive sunt deținute de compania Iridian Technologies.

Autentificarea folosind irisul ochiului este cea mai precisă dintre autentificările biometrice.

Toate sistemele de autentificare biometrice au un indicator numit Hamming Distance, pe scurt HD şi două rate de eroare ce se iau în calcul, numite False Reject Rate şi False Accept Rate, prescurtate FRR, respectiv FAR.

Indicatorul HD ne arată cu cât diferă între ele două înregistrări, de la doi irişi. Concret, dacă HD este 0.30, atunci cei doi irişi diferă în proporție de 30%.

FRR se produce atunci când setul de date obținut prin scanarea unei persoane nu se potriveşte cu nici unul memorat anterior. FAR este rata ce măsoară autentificările greşite, adică două seturi de date apropiate ca valori sunt declarate ca fiind identice, deşi nu sunt. Valoarea pentru care cele două rate sunt egale se numeşte Crossover Error Rate, prescurtat CER, iar cu cât aceasta este mai mică, cu atât sistemul este mai precis. Pentru HD<CER două seturi de date sunt considerate egale. În tabelul de mai jos, este prezentat HD, probabilitățile celor două rate de eroare şi este pusa în evidență CER:

HD	FAR	FRR
.30	1 la 6,2 miliarde	1 la 46 000
.31	1 la 665 milioane	1 la 95 000
.32	1 la 81 milioane	1 la 201 000
.33	1 la 11 milioane	1 la 433 000
.34	1 la 1,7 milioane	1 la 950 000
.342	***1 la 1,2 milioane***	***1 la 1,2 milioane***
.35	1 la 295 000	1 la 2,12 milioane
.36	1 la 57 000	1 la 4,84 milioane
.37	1 la 12 300	1 la 11,3 milioane

Principalele avantaje ale algoritmilor de recunoaştere a irisului sunt:

- **precizia** – asemeni unui fulg de nea fiecare iris este unic: irisul stâng este la fel de diferit de irisul drept la aceeaşi persoană, precum este de diferit de oricare alt iris al altei persoane; formarea irisului are loc în luna a şaptea de gestație şi se produce ca urmare a unui proces numit morfogeneză haotică; acest proces nu are legătură cu moştenirea genetică a individului şi probabilitatea ca două irisuri să

fie identice este 1 din 10^{78}; în plus, algoritmii nu presupun intervenția umană pentru a defini marje de acceptare ca în cazul altor algoritmi biometrici; cu toate acestea, probabilitatea ca o autentificare validă să fie respinsă este infimă 1 din 1.2 milioane de autentificări, precizia algoritmilor de recunoaştere a irisului datorându-se faptului că ei înregistrează peste 240 de grade de libertate ale unei caracteristici unice în construirea şablonului care va fi memorat/comparat;

- **stabilitatea** – aproape toate caracteristicile urmărite în algoritmii biometrici de autentificare se schimbă pe durata vieții unui om; vocea se schimbă, mâinile şi degetele cresc, trăsăturile feței se schimbă; cu toate acestea, irisul rămâne neschimbat începând de la vârsta de 1 an până la moarte; la moarte, irisul este unul dintre țesuturile care se deteriorează cel mai rapid, ceea ce conduce la utilizarea lui în medicina legală pentru a determina timpul decesului; pe deasupra, este imposibil a modifica irisul prin metode medicale fără a risca orbirea; chiar şi persoanele oarbe pot fi scanate atât timp cât ochiul lor are iris.
- **viteza algoritmilor** – nici un alt algoritm biometric nu oferă un grad de căutare de 1 la n într-o bază de date mare; dimpotrivă, algoritmii de autentificare, care folosesc amprenta degetului, întâmpină probleme atunci când baza de date este mare, iar pe deasupra s-ar putea să întoarcă mai mult de o singură amprentă ca posibilă pereche a celei căutate.

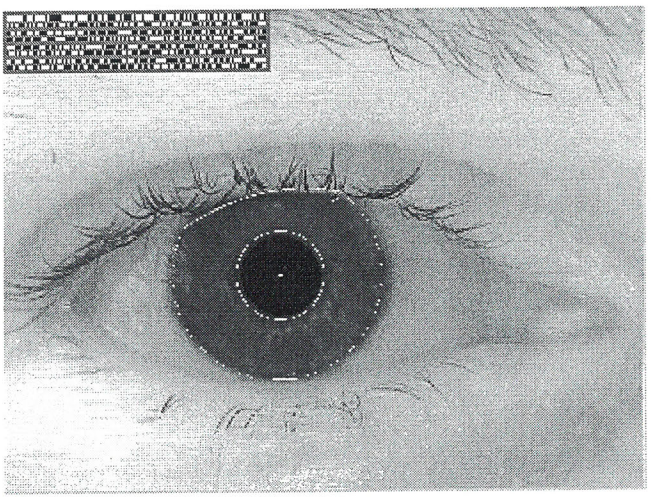

Figura 6. Iris şi amprenta irisului

- **scalabilitate** – algoritmii de recunoaştere a irisului pot fi folosiți aproape în orice aplicație de autentificare, stocarea unui iris în baza de date necesită doar 512 bytes lucru extrem de convenabil în cazul bazelor de date foarte mari;
- **nedăunător** – nu sunt folosite lumini puternice sau raze laser pentru captarea imaginii; utilizatorul poate sta până la 25 de cm distanță de receptor, poate chiar purta ochelari sau lentile de contact fără a compromite calitatea imaginii captate; spre deosebire de autentificarea folosind amprenta, nu este necesar contactul direct, ceea ce permite utilizarea algoritmilor de recunoaştere a irisului şi în acele medii în care utilizatorii poartă mănuşi.

Securizarea sistemului se face prin intensificarea sau diminuarea luminii la care este supus ochiul şi verificarea dilatării pupilei.

Autentificarea folosind retina, cronologic vorbind, este printre cele mai vechi metode folosite pentru autentificarea biometrică. Ideea acestui tip de identificare a apărut în anii '30, atunci când s-a lansat teoria conform căreia dispunerea vaselor capilare din retină este distinctivă pentru fiecare individ. Pornind de la această premisă, primul scanner de retină, denumit Eyedentification, a fost patentat în anul 1984 de compania EyeDentify. Chiar şi în ziua de astăzi, compania EyeDentify este prima pe piață.

Scanarea retinei presupune existența unui dispozitiv de captare, ce foloseşte un fascicul de lumină de intensitate scăzută, care practic face o hartă a vaselor de sânge ce vascularizează retina. Pentru a putea să se realizeze o scanare corectă, este necesar ca persoana ce se identifică să se afle la o distanță mică față de dispozitiv şi să privească printr-o fantă într-un anumit punct. De asemenea, persoanele care poartă ochelari vor fi nevoite să îi dea jos în momentul scanării. Întregul proces de autentificare durează între 10 şi 15 secunde.

Avantajele acestui tip de autentificare sunt securitatea şi acuratețea extrem de ridicate. Este foarte greu dacă nu chiar imposibil să copiezi o retină, ținând cont de faptul că modelul vascular existent pe tot

parcursul vieții se pierde o dată cu decesul individului. Datorită faptului că retina se deteriorează foarte repede în momentul în care circulația sângelui prin vase se întrerupe, nu trebuie luate măsuri suplimentare pentru a securiza dispozitivele de autentificare.

Datorită atuurilor pe care le-am enumerat mai sus, scanarea retinei este folosită pentru autentificarea accesului în instituții cu securitate ridicată cum ar fi complexe militare sau centrale electrice.

Există însă şi dezavantaje ale acestui tip de tehnologie, cum ar fi costul ridicat al dispozitivelor necesare autentificării. Unele persoane consideră că această tehnologie ar fi dăunătoare organismului, ochiului, în special, şi o consideră ca fiind prea complicată, în general.

4. Fotografia digitală şi modelele vasculare

Autentificarea cu portretul uman reprezintă un progres datorat dezvoltărilor din teoria recunoaşterii formelor.

Deşi intens mediatizată, abia după evenimentele din 11 septembrie 2001, identificarea pe baza portretului uman a fost introdusă pe piață în anii '90, iar cercetarea în domeniu a început chiar cu 10 ani înainte de introducerea ei pe piață.

Autentificarea cu portretul uman presupune captarea imaginii feței umane şi compararea ei cu şabloane deja existente.

Algoritmii actuali de recunoaştere a feței umane înregistrează anumite regiuni din fața umană, cum ar fi zona ochilor sau a nasului. Deşi prezintă încă neajunsuri, algoritmii de recunoaştere a feței umane au devenit atât de performanți încât pot recunoaşte o față chiar dacă individul este oarecum deghizat purtând ochelari sau mustață şi chiar dacă individul nu priveşte direct spre cameră.

Principalul avantaj al algoritmilor de recunoaştere a feței umane este acela că reprezintă o metodă de autentificare noncontact fiind mai uşor acceptată de utilizatori.

Autentificarea feței umane este foarte răspândită în marile corporații cu sedii distribuite în diferite locații, pentru accesul propriilor angajați, cât şi ai eventualilor contractori.

Încă la început, autentificarea feței umane poate avea un rol important în a găsi părinții eventualilor copii rătăciți în marile parcuri de distracții. Scenariul care ar permite acest lucru este următorul. Părinții împreună cu copii fac o poză când intră în parc şi îşi lasă informații de contact. Dacă este găsit un copil rătăcit în parc, iar acesta, din diferite motive, nu este capabil să-şi spună numele, atunci imaginea feței sale este comparată cu cele existente în baza de date, aflând astfel informațiile de contact ale părinților.

Pentru a creşte securitatea, multe sisteme de autentificare pe baza portretului uman necesită ca persoana ce se identifică trebuie să demonstreze că nu poartă o mască, făcând unele gesturi sau mişcări, să clipească ori să zâmbească.

Dacă această metodă de tipul noncontact reprezintă un avantaj, ei bine el este şi un impediment. Oamenii se tem că într-un viitor foarte apropiat, datorită tehnologiei de identificare pe baza portretului uman, nu vor mai avea libertate şi vor fi monitorizați la tot pasul. Cu toate acestea, tehnologia aceasta este încă departe de perfecțiune şi se încearcă constant îmbunătățirea algoritmilor de recunoaştere facială.

Inventatorul **autentificării folosind geometria palmei** a fost Sir William Herschel, magistratul şef al districtului Hooghly, din Jungipoor India. Sătul de înşelătoriile şi lipsa de onestitate a localnicilor, Sir William i-a solicitat partenerului său de afaceri indian Rajyadhar Konai parafarea unui contract prin imprimarea cu cerneală a mâinii pe spatele documentului. Bineînțeles că la acea dată, Sir William nu avea intenția de a-l identifica pe partenerul său prin acea urmă a palmei, dar în ziua de azi identificarea folosind palma este des întâlnită. Şi este folosită cu succes de peste 20 de ani.

Tehnologia aceasta presupune măsurarea şi analiza formei mâinii unei persoane. Deoarece mâna nu este unică, spre deosebire de iris sau amprentă, metoda aceasta se foloseşte mai mult cu scopul verificării identității, şi nu al autentificării efective a unui utilizator.

Partea de hardware presupune o suprafață de metal, prevăzută cu nişte semne de ghidare, care aşează mâna pentru a fi în cea mai bună poziție în momentul scanării. Compararea datelor cu cele stocate deja nu durează, de obicei, mai mult de 5 secunde.

Securizarea unor astfel de sisteme este destul de greu de realizat, deşi la prima vedere integrarea unui senzor care să detecteze dacă mâna respectivă este reală, formată din țesuturi vii, pare facilă. Un element de securitate prevăzut de astfel de sisteme este presiunea cu care se apasă asupra scanner-ului.

După cum am precizat, metoda aceasta este recomandată mai mult pentru a fi folosită în scopuri de verificare, şi nu de autentificare deoarece nu este îndeajuns de precisă, generează identificări greşite mult mai uşor decât autentificarea prin amprentă sau iris. Dacă există leziuni ale palmei, acest lucru face şi mai dificilă identificarea corectă.

Autentificarea folosind modele vasculare este încă în stadiul de cercetare. Se numără printre cele mai noi tehnologii în domeniul autentificării biometrice.

Metoda se bazează pe teoria conform căreia dispunerea şi grosimea venelor unei persoane reprezintă un model ce îl poate identifica în mod unic pe utilizatorul sau administratorul unei baze de date distribuite.

Obţinerea datelor pentru autentificare se face cu ajutorul unui scanner cu infraroşu. Teoria spune că modelul vascular este propriu unei persoane atât în zona feţei, cât şi în zona palmei, dar, din motive de implementare în practică, se foloseşte scanarea palmei.

În prezent, acest tip de autentificare este puţin folosit, dar este testat în diverse complexe militare.

Printre avantaje se numără securitatea ridicată, datorată faptului că este foarte greu să creezi o copie a unui model vascular, şi gradul ridicat de precizie, ce se estimează a-l avea metoda, deoarece venele nu sunt aşa de uşor afectate de leziuni şi condiţii externe.

Un dezavantaj dovedit este complexitatea echipamentului necesar scanării, iar alte neajunsuri care sunt încă supuse procesului de studiu ar fi efectele pe care le au asupra sistemului vascular îmbătrânirea, artrita, infarctul sau alte probleme medicale de acest fel.

Autentificarea folosind semnătura este folosită in mod curent de fiecare dintre noi, deşi de multe ori nici nu ne dăm seama.

Semnătura este, în momentul de faţă, cel mai răspândit mod de a parafa un document. Toate documentele oficiale sau nu necesită a fi semnate de către persoana autorizată pentru a-şi exprima acceptul cu privire la conţinutul lor. În lumina acestor fapte, devine evident că o metodă de autentificare, bazată pe semnătură digitală, ar fi mult mai uşor acceptată de către opinia publică.

Procesul de autentificare presupune câţiva paşi: digitizarea semnăturii, preprocesarea care constă în codarea datelor după un algoritm şi aducerea lor la o formă standard, identificarea şi extragerea informaţiilor cheie din setul de date, compararea semnăturii cu cele din baza de date şi pasul decisiv: acordarea sau neacordarea drepturilor de acces.

Semnătura este introdusă în sistem prin intermediul unui touchpad care este, de fapt, un ecran cu senzori. O metodă mai puţin răspândită este de a semna pe hârtie, în acest fel compararea semnăturilor rezumându-se la a compara două imagini. După efectuarea procesului de comparare, se va returna un număr real între 0 şi 1. O semnătură autentică va returna valori între 0,9 şi 0,95, în timp ce un fals va înregistra o valoare sub 0,7. Acesta este unul dintre tipurile de autentificare folosind semnătura şi se bazează pe un sistem capabil să „înveţe" prin prezentarea mai multor semnături atât autentice, cât şi false.

Avantajul major al acestui sistem este că nu necesită calculatoare foarte performante, pe care să ruleze (a fost testat cu succes pe un Pentium 2 rulând la 100 MHz), având nevoie de puţin spaţiu pentru stocarea datelor.

Autentificarea folosind semnătura a fost deja implementată în diverse domenii unde există nevoia de securizare a accesului. Tehnologia numită Cyber-Sign este folosită, în prezent, pentru a securiza accesul la diverse zone din interiorul Universităţii din Japonia. Această tehnologie foloseşte, de asemenea, un touchpad pentru înregistrarea semnăturilor, iar procesul de comparare a două semnături ia în calcul forma, viteza, presiunea cu care se apasă pe suprafaţa dispozitivului, precum şi timpul necesar efectuării semnăturii. Spaţiul de stocare pe care îl necesită un set de date nu este nici el mare, 1500 de bytes. Având în spate toate avantajele pe care le-am enumerat mai sus, tehnologia aceasta se poate impune într-o serie de alte domenii în viitorul apropiat.

5. Autentificarea vocală

Presupune captarea vocii unei persoane – caracteristicile fizice ale tractului vocal precum şi consonanţa şi rezonanţa – compararea ei cu amprentele vocale înregistrate într-un proces precedent. Acest tip de tehnologie prezintă interes deosebit în securizarea aplicaţiilor care necesită operaţii repetate şi unde un număr mare de persoane trebuie autentificat. Aceste sisteme includ reţele distribuite şi sisteme de acces, resetare de parole, înregistrarea timpului şi cuantificarea audienţei. Sectoarele în care se aplică sunt: serviciile financiare, aplicarea legii precum şi sănătate.

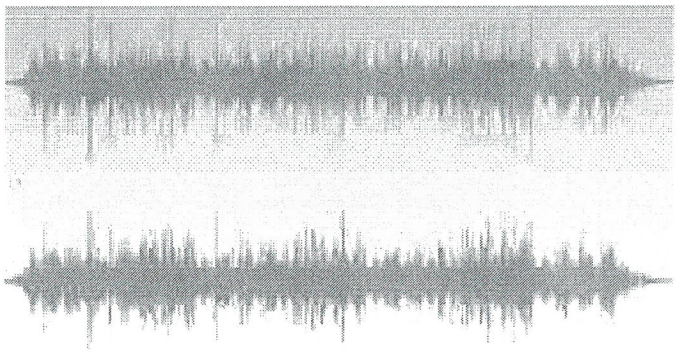

Figura 7. Amprenta vocală

Problemele cu care se confruntă algoritmii de autentificare vocală sunt: vocea care este una dintre cele mai puțin precise caracteristici biometrice, înregistrarea ei fiind dependentă atât de echipament, cât și de mediul în care se face înregistrarea. Problema este cu atât mai mare atunci când în procesul de înregistrare se folosește un echipament diferit de cel care va fi folosit în procesul de autentificare.

Pe de altă parte, autentificarea vocală are foarte mult de oferit. Pentru a autentifica utilizatorii *remote*, ei au nevoie doar de un telefon eliminând astfel restricția de a se afla într-o locație fixă unde să se autentifice.

Autentificarea vocală include două niveluri: unul este amprenta vocală, iar al doilea nivel îl reprezintă o frază cheie ce trebuie rostită. În acest caz, autentificarea vocală este combinată cu recunoașterea vocală pentru a interpreta ce a spus acel utilizator.

Pentru moment, autentificarea vocală nu are o răspândire foarte largă, ea înregistrând mai puțin de 5% din totalul afacerilor care utilizează autentificare biometrică.

Pe lângă autentificarea biometrică, apărută relativ recent în peisajul securității accesului la baze de date distribuite, există și diferite modalități de identificare, folosite de ani buni, și care au devenit deja clasice. Una dintre acestea este prezentată mai jos.

6. Autentificarea pe bază de card magnetic

Constă în recunoașterea unui cod recepționat de un cititor la apropierea unui card magnetic. Cititoarele pot fi fără memorie, doar citind codul și transmițându-l la un sistem care are înmagazinată mulțimea codurilor valide, cu memorie proprie mulțimea codurilor valide fiind stocată în dispozitiv.

Avantajele autentificării folosind cardurile magnetice sunt:

- convenienta – autentificarea este mai ușoară decât a tasta un cod sau a-ți scana una din caracteristicile biometrice: amprentă, voce, iris, față;
- cost redus – echipamentele și aplicațiile utilizate în autentificarea folosind carduri magnetice au un cost mult mai mic decât cele care folosesc caracteristici biometrice;
- rapiditate – căutarea în baze de date foarte mari este extrem de rapidă de obicei făcându-se pe o cheie numerică.

Cu toate acestea, autentificarea folosind carduri magnetice prezintă marele dezavantaj că autentificarea este a cardului, și nu a persoanei, ceea ce se traduce prin două inconveniente: lipsa cardului implică utilizarea altui mecanism de autentificare și faptul că o altă persoană care se află în posesia cardului, îl poate folosi pentru a se autentifica. Pentru a înlătura acest neajuns în sistemele în care autentificarea individului este importantă, cardurile magnetice se folosesc în combinație cu autentificarea folosind caracteristici biometrice. Nu mai sunt o noutate cardurile magnetice care includ o zonă pentru scanarea amprentei degetului. De asemenea, la accesul în clădiri, de obicei, se află și o cameră video.



Figura 8. Cititor cu memorie

Autentificarea folosind cardurile magnetice este foarte răspândită la hoteluri, în sisteme de pontaj, parcări, acces în instituții.

Multe țări se gândesc serios la un proces de singularizare a autentificării folosind cardurile magnetice în combinație cu caracteristicile biometrice. Obiectivul este acela de a exista un sigur card per individ, care să înlocuiască toate celelalte metode de autentificare: buletinul de identitate, carnetul de conducere, paşaportul, codul unic personal, cardurile de credit/debit, cardurile de asigurare de sănătate şi cardurile de acces în clădiri.

7. Sistem de contabilitate distribuit

Necesitățile implicate de sistem constau în:

- o listă de ipoteze;
- o schemă de realizare a întregului ansamblu server-clienți;
- modalități de autentificare;
- existența unui server şi a mai multor utilizatori care închiriază spații pe respectivul server şi stochează date şi rezultate în partiții protejate.

În cadrul acestui sistem, toți utilizatorii folosesc de la distanță acelaşi software, prin intermediul căruia accesează datele stocate pe server.

Autentificarea este utilizată pentru:

- a avea acces la sistemul de prelucrare;
- a avea acces la baza de date;
- a realiza o serie de operații pe baza de date: consultare, adăugare de date.

Avantajele acestui sistem sunt:

- nu mai este necesar ca fiecare utilizator să aibă propriul software;
- costuri reduse cu găzduirea;
- terminalele de la care se realizează accesul la server nu trebuie să fie sisteme sofisticate, serverul fiind cel care găzduieşte aplicația în sine;
- securitatea datelor;
- actualizarea în timp real a datelor, astfel încât utilizatorii beneficiază, în acelaşi timp, de aceleaşi resurse;

- siguranța stocării datelor, acestea fiind protejate prin diferite metode de back-up.

Folosirea sistemelor distribuite contribuie la îmbunătățirea accesului la date prin stocarea aplicațiilor de gestiune direct pe server, clientului fiindu-i necesară o configurație software minimă, și prin înlăturarea dependenței existente între date și locația unde sunt stocate, serverul fiind cel care oferă acces la date utilizatorilor, indiferent de locația de unde este solicitat accesul.

8. Concluzii

Toate metodele de autentificare prezintă avantaje și dezavantaje. De aceea, sistemele moderne de autentificare folosesc metode multiple de autentificare pentru a agrega avantajele și a înlătura neajunsurile.

Dezvoltarea globală a sistemului informațional își spune cuvântul și în dezvoltarea algoritmilor de autentificare. Timpurile când utilizatorul trebuia să fie în fața monitorului pentru a introduce o parolă, primind astfel acces la informația dorită se apropie de sfârșit. Noile metode de autentificare permit autentificarea în sistem chiar dacă utilizatorul este în vacanță într-o țară exotică și, eventual, a uitat parola. O frază rostită la telefon sau o imagine transmisă prin internet au același efect precum tastarea unei parole care, cel mai adesea, trebuie să fie suficient de lungă, să conțină cifre și alte caractere decât literele, făcând-o astfel greu de memorat.

Noile metode pot conduce la subțierea portofelului, și nu pentru că sunt mult mai costisitoare, ci pentru că permit încorporarea tuturor mecanismelor de autentificare digitală sau prin intervenție umană într-unul singur, mult mai convenabil de utilizat și mult mai greu de copiat.

O autentificare aproape de perfecțiune presupune trei metode agregate pentru a da o siguranță maximă. Această autentificare absolută implică îmbinarea trecutului, prezentului și viitorului, principiul enunțat fiind unul simplu și pe înțelesul oricui: ceva ce cunoaște utilizatorul/administratorul, ceva ce are și ceva ce este.

Trecutul este reprezentat de banala ***parolă*** care a fost și mai este încă cel mai răspândit mod de autentificare. Deși pare depășit și fragil, sistemul de autentificare *user-parolă* este destul de sigur. Cercetări ulterioare au impus ca obligatorii unele proceduri ușor de respectat și care oferă sistemului o securitate sporită. Una dintre cele mai simple metode de securizare a accesului cu user și parolă este obligativitatea combinării mai multor tipuri de caractere pentru a forma parola; multe autentificări de acest tip necesită ca parola să fie definită folosind litere mari, mici, cifre, dar și caractere speciale cum ar fi „#" sau „@". De asemenea, eficientă este compunerea unui user și a unei parole din mai multe seturi separate: mai multe persoane dețin propriul user și parolă, care sunt însă valabile doar în prezența tuturor celorlalte seturi user-parolă. Metoda poate fi comparată cu mai multe chei, deținute de persoane diferite, care sunt folosite pentru a deschide o ușă, dar nu funcționează decât dacă sunt rotite toate simultan.

Cardul reprezintă prezentul, fiind în momentul de față un mod foarte răspândit, utilizat pe scară largă, de autentificare și securizare a accesului în diverse instituții. Autentificarea cu cardul este folosită pentru a permite:

- accesul tuturor salariaților în instituție;
- accesul relativ: doar anumiți angajați autorizați au permisiunea de a intra în unele încăperi;
- accesul în cascadă: agregarea accesului cu cardul în încăpere cu autentificarea pe un calculator prin intermediul utilizatorului și a parolei.

Tehnologia viitorului constă în autentificarea folosind o ***dată biometrică*** a individului, iar dintre cele pe care le-am enumerat în această lucrare rămâne de văzut care se va dovedi cea mai fiabilă.

Un lucru este cert, o tehnologie care să ducă la o autentificare infailibilă nu va exista niciodată. Întotdeauna vor exista portițe de a păcăli sistemul, portițe ce vor fi exploatate de cei interesați. Dar agregarea acestor trei metode va avea ca efect creșterea exponențială a securității autentificării.

Bibliografie

1. **PATRICIU, V.V., M. ENE-PIETROŞANU, I. BICA, J. PRIESCU**: Semnături electronice şi securitate informatică, Editura All, Bucureşti, 2006.
2. **PATRICIU, V.V., M. ENE-PIETROŞANU, C. VĂDUVA, I. BICA:** Securitatea comerţului electronic, Editura All, Bucureşti, 2001.
3. **KOMARINSKI, P.**: Automated Fingerprint Identification Systems (AFIS), Academic Press, New York, 2004.
4. **WAYMAN, J., A. JAIN, D. MALTONI, D. MAIO**: Biometric Systems: Technology, Design and Performance Evaluation, Springer Verlag, Berlin, 2004.
5. [www1] **GILHOOLY, K.**: Voice Authentication: Making Access a Figure of Speech, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=86897.
6. [www2] **EASEN, N.**: Sweden tests bio-ID cards, CNN http://www.cnn.com/2003/WORLD/europe/11/25/biz.trav.sas.biometric/index.html.
7. [www3] National Center for State Courts - SJI E-Court Conference 2002, http://ctl.ncsc.dni.us/biomet%20web.
8. [www4] **MANOLESCU, M. C.**: Signature Recognition Project, 1996 http://bip.golana.pub.ro/~mmihai/sign/.
9. [www5] CyberSign - Technology Overview, http://www.cybersign.com/techoverview.htm.